ZoneAlarm security software

User Guide

version 9

ZoneAlarm by Check Point

August 24, 2009

© 2009 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

©2003–2009 Check Point Software Technologies Ltd. All rights reserved.

Please refer to **http://www.checkpoint.com/copyright.html** for a list of our trademarks.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Contents

Welcome ix

About this guide ix
Guide Conventions ix
ZoneAlarm User Forum x
ZoneAlarm Readme x

Chapter 1 ZoneAlarm security software basics 1

Tour of the ZoneAlarm control center 1
Tour of main features. 2
About the Overview panel 4
Viewing your protection statistics 5
System tray icons and shortcut menus 7

Responding to alerts 8

Firewall zone basics 10
Zones manage firewall security 10
Zones provide program control as outbound protection 11

Configuration basics 12

Setting product preferences 13
Setting product update options 14
Setting your password 14
Backing up and restoring your ZoneAlarm settings 15
Setting general product preferences 15
Setting contact preferences 16
Setting product display and proxy server options 17
Creating an online fraud protection profile 17

Licensing, registration, and support 18
When your license expires. 18
Renewing your product license 19
Accessing technical support 19
Updating your ZoneAlarm registration information 20

Updating and upgrading your product 20
About updating from a prior version 20
Upgrading to another ZoneAlarm product 20

Uninstalling ZoneAlarm 21

Moving to a different computer 21

Chapter 2 Configuring for networks and resources 23

Configuring a new network connection 23
Using the Network Configuration Wizard 24

Disabling the Network Configuration Wizard . . . 24
Using the Wireless Network Configuration Wizard . . . 25
Disabling the Wireless Network Configuration Wizard . . . 25
Integrating with network services . . . 26
Enabling file and printer sharing . . . 26
Connecting to network mail servers . . . 27
Enabling Internet Connection Sharing . . . 27
Configuring your VPN connection . . . 27
Supported VPN protocols . . . 28
Configuring your VPN connection automatically . . . 28
Configuring your VPN connection manually . . . 29
Adding a VPN gateway and other resources to the Trusted Zone . . . 30
Removing a VPN gateway from a blocked range or subnet . . . 30
Allowing VPN protocols . . . 30
Granting access permission to VPN software . . . 31

Chapter 3 Firewall protection . . . 33

Understanding Firewall protection . . . 33
Choosing security levels . . . 34
Setting the security level for a Zone . . . 34
Setting advanced security options . . . 35
Setting gateway security options . . . 36
Setting ICS (Internet Connection Sharing) options . . . 36
Setting general security options . . . 36
Setting network security options . . . 38
Setting wireless network security options . . . 38
Managing traffic sources . . . 39
Viewing the traffic source list . . . 39
Modifying traffic sources . . . 40
Adding to the Trusted Zone . . . 40
Adding to the Blocked Zone . . . 42
Viewing logged Firewall events . . . 42
Blocking and unblocking ports . . . 43
Default port permission settings . . . 43
Adding custom ports . . . 44
Understanding expert firewall rules . . . 46
How expert firewall rules are enforced . . . 46
Expert firewall rule enforcement rank . . . 47
Creating expert firewall rules . . . 48
Creating groups . . . 50
Creating a location group . . . 50
Creating a protocol group . . . 51
Creating a day/time group . . . 53
Managing Expert Firewall Rules . . . 54
Viewing the Expert Rules list . . . 55
Editing and re-ranking rules . . . 56

Chapter 4 Understanding and reducing alerts 59

About alerts and managing them 59

Informational alerts 60
Firewall alerts/Protected 61
MailSafe alert 62
Blocked Program alert 63
Internet Lock alert 64
Remote alert 65

Program alerts 65
New Program alert 68
Repeat Program alert 69
Changed Program alert 69
Program Component alert 70
Server Program alert 71
Advanced Program alert 73
Automatic VPN Configuration alert 74
Manual Action Required alert 74

OSFirewall alerts 75
Medium-rated Suspicious Behavior alert 75
High-rated Suspicious Behavior alert 77
Malicious behavior alert 81

ID Lock alert 82

New Network alerts 83

Chapter 5 Program Control 89

Understanding Program Control 89
Setting program permissions automatically 90
Setting program permissions manually 91

Setting general program control options 93
Setting the program control level 93
Custom program control features 95
Configuring OSFirewall protection 96
Understanding services control 96
Enabling Component Control 97
Setting the SmartDefense Advisor level 98
Enabling the automatic lock 98
Viewing logged program events 100
Viewing logged OSFirewall events 101

Setting permissions for specific programs 101
Using the programs list 102
Adding a program to the programs list 105
Granting a program permission to access the Internet 106
Granting a program permission to act as a server 106
Granting send mail permission to a program 107

Setting program options for a specific program 107
Setting Advanced Program Control options 108
Disabling Outbound Mail protection for a program 108
Setting Filter options for a program 109
Setting authentication options 109

Setting passlock permission for a program . . . 109
Managing program components . . . 110
Creating expert rules for programs . . . 111
Creating an expert rule for a Program . . . 112
Sharing expert rules . . . 112

Chapter 6 ZoneAlarm browser security . . . 117

Using ZoneAlarm browser security . . . 117

Chapter 7 Virus and spyware protection . . . 120

Spyware and virus Protection . . . 120
Turning on virus and spyware protection . . . 121
Scheduling regular scans . . . 121
Keeping virus definitions up-to-date . . . 121
Customizing virus protection options . . . 122
Specifying scan targets . . . 123
Choosing a scan mode . . . 124
Configuring on-access scanning . . . 125
Enabling automatic virus treatment . . . 126
Specifying scan options . . . 127
Excluding items from virus scans . . . 127
Performing a scan . . . 129
Understanding virus scan results . . . 130
Treating virus files manually . . . 131
Repairing files in an archive . . . 132
Submitting viruses and spyware to ZoneAlarm for review . . . 132
Viewing logged virus events . . . 133
Viewing items in quarantine . . . 134
Viewing virus and spyware protection status . . . 135
Monitoring virus protection . . . 136
Monitoring Coverage . . . 136
Monitoring product status . . . 137
Monitoring antivirus status alerts . . . 137
Enabling and disabling Anti-virus Monitoring . . . 137
Viewing Status Messages in the Anti-virus Monitoring panel . . . 137

Chapter 8 Parental Controls . . . 139

Using Parental Controls . . . 139
Working with parental controls and smart filtering . . . 139
Choosing which content categories to block . . . 141

Chapter 9 E-mail protection . . . 147

Understanding e-mail protection . . . 147
Outbound MailSafe protection . . . 148
Enabling Outbound MailSafe protection . . . 148
Customizing Outbound MailSafe protection . . . 148

Enabling Outbound MailSafe protection by program 148
Setting Outbound MailSafe protection options 149

Filtering junk e-mail (spam) 150
Allowing or blocking e-mail from specific senders 151
Allowing or blocking e-mail from specific companies 151
Adding contacts to the Allowed List 151
Scanning your Inbox 151
Allowing e-mail from distribution lists 152
Reporting junk e-mail 152
Reporting phishing e-mail 153
Specifying junk e-mail message options 154
Challenging e-mail from unknown senders 155
Specifying your outbound e-mail server 156
Customizing junk e-mail filter settings 156
Restoring e-mail incorrectly identified as junk 158
Viewing junk e-mail filter reports 158

Chapter 10 Identity protection 160

Understanding the ID Lock feature 160
How your personal information is protected 161
Setting the ID Lock protection level 162

About myVAULT 163
Adding data to myVAULT 163
Editing and removing myVAULT contents 165

Using the Trusted Sites list 166
Viewing the Trusted Sites list 167
Adding to the Trusted Sites list 168
Editing and removing trusted sites 168

Identity Protection Center 168

Chapter 11 Hard Drive Encryption for Laptops 172

Do I need Hard Drive Encryption for Laptops? 172

Using Hard Drive Encryption for Laptops 173

Installing Hard Drive Encryption for Laptops 174

Hard Drive Encryption Main panel 175
Creating your recovery disk 175
The Encryption Status bar 176

Hard Drive Encryption Advanced panel 176
Stopping or removing Hard Drive Encryption 177

Troubleshooting Hard Drive Encryption 177
What to do if you forget your password or username: 178
How to decrypt in case of system failure 178

Chapter 12 Managing Alerts and Logs 181

Understanding alerts and logs 182

Setting basic alert and log options 182

Setting the alert event level 183
Setting event and program logging options. 183
Controlling the number of alerts 183
Showing or hiding firewall and program alerts 184
Setting event and program log options 184
Formatting log appearance 184
Customizing event logging 185
Customizing program logging 185
Viewing log entries 186
Viewing the text log 188
Archiving log entries 190
Using SmartDefense Advisor and Hacker ID. 191

Chapter 13 Game Mode 193
Understanding Game Mode 193
Turning Game Mode On and Off 194

Appendix N Troubleshooting 197
VPN 197
Configuring ZoneAlarm security software for VPN traffic 198
VPN auto-configuration and expert rules 198
Automatic VPN detection delay 198
Networking 199
Making your computer visible on your local network 199
Sharing files and printers across a local network 199
Resolving a slow start up 200
Internet Connection 200
Connecting to the Internet fails after installation 201
Allowing ISP Heartbeat messages 201
Connecting through an ICS client. 202
Connecting through a proxy server 202
Unable to connect to program advice server 202
Anti-virus 203
If a safe application has been quarantined. 203
Anti-virus Monitoring alert 204
Resolving conflicts with anti-virus products 204
E-mail scanning is unavailable 204
Hard Drive Encryption 205
Third-party software 205
Anti-virus 206
Browsers 206
Chat and instant messaging programs 206
E-mail programs 207
Internet answering machine programs 207
File sharing programs 207
FTP programs 208
Games 208
Remote control programs 209

VNC programs 210
Streaming media programs 210
Voice over IP programs 211
Web conferencing programs 211

Appendix O **Keyboard shortcuts** 215

Navigation shortcuts 215

Global function shortcuts 216

Dialog box commands 217

Button shortcuts 218

Glossary 222

Index 234

Welcome

Welcome to ZoneAlarm, the easy-to-use Internet security software that protects you from known and unknown threats.

Quick Links:

- **Tour of main features**
- **Troubleshooting**

Topics:

- "About this guide," on page ix

About this guide

Throughout this guide all ZoneAlarm security software products are collectively referred to as ZoneAlarm security software.

This online help documents all possible features in the ZoneAlarm security software products, though not all features are in all products.

- Guide Conventions
- ZoneAlarm User Forum
- ZoneAlarm Readme

Guide Conventions

This guide uses the following formatting and graphics conventions.

Convention	Description
|	Used to separate panel selections in procedures. Shows navigation path. Example: Select **Firewall** | **Zones**, then click **Add**.
	Note icon. Emphasizes related, reinforcing, or important information.

Convention	Description
	Caution icon. Indicates actions or processes that can potentially damage data or programs.

ZoneAlarm User Forum

Connect with other users of ZoneAlarm security software. Ask questions, get answers, and see how fellow users get the most out of their ZoneAlarm security software. Visit: **http://www.zonealarm.com/security/en-us/community/user-forum-agreement.htm**

ZoneAlarm Readme

System requirements and known issues and workarounds can be found in the Readme document.

To open the Readme, from the Windows **Start** menu, choose **Programs | ZoneAlarm | Readme**.

Chapter 1

ZoneAlarm security software basics

ZoneAlarm is pre-configured to provide protection as soon as you install it, and will alert you if it needs anything from you. This chapter provides an introduction to the main tools and concepts of ZoneAlarm security software.

Topics:

- "Tour of the ZoneAlarm control center," on page 1
- "Firewall zone basics," on page 10
- "Configuration basics," on page 12
- "Setting product preferences," on page 13
- "Licensing, registration, and support," on page 18
- "Updating and upgrading your product," on page 20
- "Uninstalling ZoneAlarm," on page 21
- "Moving to a different computer," on page 21

Tour of the ZoneAlarm control center

If ZoneAlarm security software is installed and running, there is nothing you need to configure in order to start being protected— it alerts you if it needs tell you or ask you anything. When you want to explore the features and your options, the control center provides one-stop access. The major features are presented in a menu on the left side of the control center, and described in the section that follows.

- Tour of main features
- About the Overview panel

- Viewing your protection statistics
- System tray icons and shortcut menus

Tour of main features

To move from feature to feature, select the feature you want from the Navigation bar.

Features in the Navigation Bar

Each item you see in the Navigation bar represents a main feature in the product. Click a feature to display all panels and subpanels for that feature.

Some features listed below may not be included in your version of the product.

Navigation item	Feature Description
Overview	This panel tells you at a glance if your computer is secure. You can also get a summary of protection activity and see if your product is up to date, and access or download additional Web-based services like backup and system tune-up (in some versions). For more details, see "About the Overview panel," on page 4.
Inbound Firewall	Protects your computer from dangerous intrusions by guarding the "doors" (network ports) to your computer. The default settings defend you against unauthorized intrusions. Advanced users can customize firewall configurations. For more information, see Chapter 3,"Firewall protection," starting on page 33.
Program Control	Protects you against criminal programs that would send your personal data over the Internet. Ensures that only programs you trust access the Internet. Also, OS Firewall alerts you if programs try to perform suspicious actions. If ZoneAlarm does not recognize a program, it asks you what access you want to give to it. For more information, see Chapter 5,"Program Control," starting on page 89.
Anti-virus and Antispyware	Detects and treats malicious programs called viruses and spyware. Checks your system against constantly updated databases of known viruses and spyware. Detects virus or spy-like behaviors such as self-modifying, self-replicating, data capturing, and port altering. For more information, see Chapter 7,"Virus and spyware protection," starting on page 120.
Parental Controls	The Parental Controls let you block Web sites containing undesired content. You can choose which categories to block, and use Smart Filtering to instantly categorize and filter previously un-rated sites. For more information, see Chapter 8,"Parental Controls," starting on page 139.
Browser Security	ZoneAlarm ForceField protects your personal data, privacy, and your PC while you are on the Web. You will see ForceField browser toolbar and border around the edge of browser. Defends against drive-by downloads, browser exploits, phishing, and spyware. Includes a Private Browser option that "leaves no trace" behind on your computer. See "Using ZoneAlarm browser security," on page 117,
E-mail Protection	Protects the people in your e-mail address book by halting outbound email that displays virus-like activity. The Junk E-mail Filter removes unwanted spam mail from your inbox, and can prevent identity theft by deleting phishing email. For more information, see Chapter 9,"E-mail protection," starting on page 147.

Table 1-1: Explanation of navigation bar features

Navigation item	Feature Description
Identity Protection	You can put your personal data into a virtual "vault" (called myVAULT) to keep it safe from hackers and ID thieves. Then set Identity Lock to Medium or High to protect your vault data. Some versions of the product also include a button for signing up for offline identity protection. For more information, see Chapter 10,"Identity protection," starting on page 160.
Hard Drive Encryption	Locks your entire disk with special encryption so that laptop thieves cannot access it. See Chapter 11,"Hard Drive Encryption for Laptops," starting on page 172. This panel only appears if you install Hard Drive Encryption.
Alerts and Logs	This panel helps you control how many pop-up alerts you see and which alerts are logged. For more information, see Chapter 12,"Managing Alerts and Logs," starting on page 181.

Table 1-1: Explanation of navigation bar features

QuickTasks

The **QuickTasks menu** saves you steps by going directly to the window or dialog relevant to the task.

Check for Updates makes sure that your product features and anti-virus/spyware signature database are both up-to-date. If they are not up-to-date, the proper updates are downloaded and installed automatically.

About Online Help

To go to the Help Center, which includes Tutorial and Troubleshooting links, click **Quick Tasks | Help | Help Center**.

To get Help on the panel you are currently viewing choose **Quick Tasks | Help | About this Panel** or press **F1.**

Related Topics:

- About the Overview panel
- Viewing your protection statistics
- System tray icons and shortcut menus

About the Overview panel

The Overview panel tells you whether your security settings are enabled and provides a summary of security activity.

From the Overview panel you can:

- *Confirm Protection:* See at a glance if your computer is secured by all default ZoneAlarm security software protections:
  - **Green** means all default protections are on.
  - **Red** means a default security feature is off. Click **Fix It** to turn it back on and restore default settings.
- *Protection Statistics:* Click "See how" or a green button to see how the product has been protecting you, as described in "Viewing your protection statistics," on page 5.
- *Additional Services:* Access services, such as Identity Protection and online backup, which are included in some versions of ZoneAlarm. (If you don't see these features on the right side of the window, you can purchase them at www.zonealarm.com.) Some Additional Services buttons guide you in installing the services first. After the service is installed, just click the same Additional Services button to launch the service.

When you purchase ZoneAlarm security software, you receive an *automatic product update subscription* valid for one year, which means that when an updated version of your product is released, your software notifies you and you can download it instantly for free.

Your ZoneAlarm security software will keep you aware of the status of your subscription. See also "Renewing your product license," on page 19.

Viewing your protection statistics

To view statistics and details on how ZoneAlarm security software has been protecting you do either of the follow:

- Click one of the **green buttons** in the middle of the Overview panel
- Click the **See how...** link above the green buttons

Depending on which version of ZoneAlarm security software you are running, the **Protection Details** window displays the some or all of the following information:

Firewall Security

Depending on which version of ZoneAlarm security software you are running, this area displays some or all of the following data:

- *Inbound Firewall:* Shows you how many times the ZoneAlarm security software firewall and has acted to protect you, and how many were *high-rated alerts*.
- *Outbound Firewall:* Indicates how many programs have been secured for appropriate access to the Internet.

- *O/S Firewall:* Indicates whether the Operating Firewall system is on and whether any suspicious behaviors have been detected.

Anti-virus and Anti-spyware Security

Depending on which version of ZoneAlarm security software you are running, this area displays some or all of the following data:

- *Anti-virus/Anti-spyware Protection:* Indicates whether your computer is protected against malware and displays treatment statistics. If you are using a version of the product that doesn't include this protection, you will see Anti-virus Monitoring status instead.

Browser Security

Depending on which version of ZoneAlarm security software you are running, this area displays some or all of the following data:

- *Virtual Browsing Security:* Shows how many Web browsing sessions have been secured by ForceField.
- *Anti-phishing and Malware Protection:* Displays number of dangerous sites detected and number of Web downloads scanned.

System tray icons and shortcut menus

The icons displayed in the system tray let you monitor your security status and Internet activity as frequently as you wish, and access your security settings in just a few clicks

System tray icons

Icon	Description
	ZoneAlarm security software is installed and running.
	Your computer is sending (red band) or receiving (green band) network traffic. This does not imply that you have a security problem, or that the network traffic is dangerous.
	ZoneAlarm security software is running a spyware and/or virus scan. For details about scans, see “Performing a scan,” on page 129.
	Game Mode is activated, causing ZoneAlarm security software to suppress feature and anti-virus signature updates, scans, and most alerts. For details about this feature, see “Game Mode,” on page 193.
	ZoneAlarm security software is receiving an anti-virus signature update.
	(Yellow lock) The **Internet Lock** is engaged.
	(Red lock) **Stop all Internet Activity** is engaged. You may also begin to see a lot of alerts.

System tray shortcut menu

Right-click any of the system tray icons to access a shortcut menu.

Menu item	Description
Open Browser	Opens your Web browser, secured by ForceField protection.
Open Private Browser	Opens your Web browser, secured by ForceField in Private Browser mode. In this mode, no trace is left on your computer of what you've typed in your browser or sites you've visited. See the ForceField online Help (in the ForceField toolbar) for more information.
Open Unprotected Browser	Opens your Web browser without ForceField protection.
Engage Internet Lock	Engages the Internet Lock and displays the yellow lock icon in the system tray. The Internet Lock stops all traffic except traffic initiated by programs to which you have given *pass-lock* permission. Clicking the Internet Lock instantly blocks DHCP messages or ISP heartbeats used to maintain your Internet connection. As a result, you may lose your Internet connection.

Table 1-2: System Tray Shortcut Menu

Menu item	Description
Stop All Internet Traffic	Engages the Stop button and displays the red lock icon in the system tray. All Internet traffic is blocked. You should click the Stop button only if you believe your computer is under attack, otherwise, ZoneAlarm security software may block legitimate programs that require access, as well as *DHCP (Dynamic Host Configuration Protocol)* messages or ISP *heartbeat messages* used to maintain your Internet connection.
Game Mode / Stop Game Mode	Opens the dialog that controls Game Mode. When activated, Game Mode suppresses ZoneAlarm updates, scans, and most alerts. You choose whether to deny or allow all program and network permission requests while Game Mode is active. For details about this feature, see Chapter 13,"Game Mode," starting on page 193.
Help	Displays the Help Center, which includes Troubleshooting and a Tutorial link.
View Scan	Displays the Scanning Status dialog box, which tracks the progress of spyware and virus scans and allows you to pause or cancel a scan. Available only during scans.
About	Displays version information for the ZoneAlarm security software you have installed, including driver and engine information. If you are experiencing problems with your software you can copy this information to the clipboard and paste it into an e-mail to support.
Restore ...Control Center	Displays the ZoneAlarm security software Control Center at full size onscreen. The label for this menu option reflects the version of ZoneAlarm security software you have installed.
Shutdown...Control Center	Closes the ZoneAlarm security software application. The label for this menu option reflects the version of the ZoneAlarm security software you have installed.

Table 1-2: System Tray Shortcut Menu

Responding to alerts

When you first start using ZoneAlarm security software, it is not unusual to see a number of alerts. Don't worry! This doesn't mean you're under attack. It just means that ZoneAlarm security software is learning your program and network configurations, and giving you the opportunity to set up your security the way you want it.

How you respond to an alert depends upon the type of alert displayed.

To understand the different types of alerts you see, and to find out what you can do to see fewer of them, use "Understanding and reducing alerts," on page 59.

Because New Program alerts and New Network and VPN alerts are the most common alerts you may see, they are introduced here.

New Program alerts

The majority of the initial alerts you see will be New Program alerts. These alerts occur when a program on your computer requests access or server permission to the Internet or your local network. Use the New Program alert to give access permission to programs that need it—like your browser and e-mail program.

Use the check box labeled **Remember this answer** to give permanent permission to programs you trust.

Few programs or processes actually require server permission in order to function properly.

Some processes, however, are used by Microsoft Windows to carry out legitimate functions. Some of the more common ones you may see in alerts are: lsass.ex, spoolsv.exe, svchost.exe, services.exe, winlogon.exe.

Be aware that many legitimate Windows processes, including those listed above, have the potential to be used by hackers to disguise worms and viruses, or to provide backdoor access to your system for Trojan horses. So, if you were not performing a function (such as browsing files, logging onto a network, or downloading files) when the alert appeared, then the safest approach is to deny server permission. If you do not recognize the program or process that is asking for server permission, search the Microsoft Support Web site (**http://support.microsoft.com/**) for information on the process to determine what it is and what it's used for.

At any time, you can assign permissions to specific programs and services from the Programs List, accessed by selecting the **Program Control**|**Programs** panel.

To learn more about New Program alerts and how to respond to them and see fewer of them, see "New Program alert," on page 68.

New Network and VPN alerts

The other initial alerts you may see are the New Network alert and VPN Configuration alerts. These occur when ZoneAlarm security software detects a network connection or VPN connection. They help you configure your Trusted Zone, port/protocol permission, and program permissions correctly so that you can work securely over your network.

To learn more about these alerts and how to respond to them, see "New Network alerts," on page 83.

Firewall zone basics

ZoneAlarm security software keeps track of the good, the bad, and the unknown out on the Internet by using virtual containers, called Zones, to classify the computers and networks that connect to your computer.

The *Internet Zone* is the "unknown." All the computers and networks in the world belong to this Zone—until you move them to one of the other Zones.

The *Trusted Zone* is the "good." It contains all the computers and networks you trust and want to share resources with—for example, the other machines on your local or home network.

The *Blocked Zone* is the "bad." It contains computers and networks you distrust.

When another computer wants to communicate with your computer, ZoneAlarm security software looks at the Zone it is in to help decide what to do.

To learn how to put a computer, network, or program in the Trusted Zone, see "Managing traffic sources," on page 39.

- Zones manage firewall security
- Zones provide program control as outbound protection

Zones manage firewall security

ZoneAlarm security software uses security levels to determine whether to allow or block inbound traffic from each Zone. Use the **Firewall** panel to view and adjust security levels.

High security setting

High security places your computer in *stealth mode*, making it invisible to hackers. High security is the default configuration Internet Zone.

In High security, file and printer sharing is disabled; but outgoing DNS, outgoing DHCP, and broadcast/multicast are allowed, so that you are able to browse the Internet. All other ports on your computer are closed except when used by a program that has access permission and/or server permission.

Medium security setting

Medium security places your computer in *component learning mode*, where ZoneAlarm security software quickly learn the MD5 signatures of many frequently used program components without interrupting your work with multiple alerts. Medium security is the default setting for the Trusted Zone.

In Medium security, file and printer sharing is enabled, and all ports and protocols are allowed. (If Medium security is applied to the Internet Zone, however, incoming NetBIOS traffic is blocked. This protects your computer from possible attacks aimed at your Windows networking services.) At Medium security, you are no longer in stealth mode.

We recommend that you use the Medium security setting for the first few days of normal Internet use after installing ZoneAlarm security software. After a few days of normal use, ZoneAlarm security software will have learned the signatures of the majority of the components needed by your Internet-accessing programs, and will remind you to raise the Program Authentication level to High.

No security level is necessary for the Blocked Zone, because no traffic to or from that Zone is allowed.

Advanced users can customize high and medium security for each Zone by blocking or opening specific ports. For more information, see "Blocking and unblocking ports," on page 43.

Zones provide program control as outbound protection

Whenever a program requests *access permission* or *server permission*, it is trying to communicate with a computer or network in a specific Zone. For each program you can grant or deny the following permissions:

- Access permission for the Trusted Zone.
- Access permission for the Internet Zone.
- Server permission for the Trusted Zone.
- Server permission for the Internet Zone.

By granting access or server permission for the Trusted Zone, you enable a program to communicate only with the computers and networks you have put in that Zone. This is a highly secure strategy. Even if a program is tampered with, or given permission accidentally, it can only communicate with a limited number of networks or computers.

By granting access or server permission for the Internet Zone, however, you enable a program to communicate with any computer or network, anywhere.

Advanced users can specify the ports and protocols a particular program can use, the hosts it can access, and other details. For more information, see "Creating an expert rule for a Program," on page 112.

Configuration basics

The Configuration Wizard

Upon completing installation, the **Configuration Wizard** appears. The Configuration Wizard assists you in setting the basic ZoneAlarm security software options. You can use the Configuration Wizard to enable Anti-virus protection, join DefenseNet, and run a security scan of your applications and programs that helps minimize unnecessary program alerts later. The Configuration Wizard appears only after installation.

Configuring program Internet access permissions

While ZoneAlarm security software can automatically set permissions that specify which programs can transmit information across your firewall, you have the option of specifying these permissions for many of the most popular programs in the following software categories:

- Instant Messaging programs
- Web browsers
- Microsoft Office
- E-mail
- Anti-virus
- Microsoft Windows processes
- Document utilities
- ZoneAlarm software applications

For more information about assigning permission to programs, see "Setting permissions for specific programs," on page 101.

Joining the DefenseNet community

ZoneAlarm security software users can help shape the future of ZoneAlarm security products by joining the DefenseNet community protection network and periodically sending anonymous configuration data to ZoneAlarm for analysis. By joining DefenseNet, you can help us focus our attention on the features and services that you use most often and to introduce new functionality that will provide even smarter security.

Configuration data is not collected from ZoneAlarm or ZoneAlarm Anti-virus users.

Even with the "Alert me before I make contact" preference selected in the **Overview**|**Preferences** panel, you will not be alerted before sending configuration data to ZoneAlarm.

The data collected is completely anonymous and is for ZoneAlarm internal use only and will not be shared with others. Of the millions of ZoneAlarm security software users, only a small percentage of users will have their information collected. The frequency of data transmission depends upon the configuration of your computer. For most users, data will be sent once per day.

To send configuration data to ZoneAlarm, do one of the following:

- Select **Yes, automatically and anonymously share my settings** in the Configuration Wizard that appears after installation.
- Or, if you did not make this setting when the Configuration Wizard appeared, do this:
  - Select **Overview**|**Preferences**.
  - In the **Contact with ZoneAlarm** area, select Share **my security settings anonymously with ZoneAlarm**.

If you later decide that you do not want to send anonymous data, select **Overview**|**Preferences**, in the Contact with ZoneAlarm area, then clear the **Share my settings anonymously...** check box.

Product preferences

See "Setting product preferences," on page 13 to find out how to set or change your ZoneAlarm security software password, log in or log out, manage product feature updates (but not virus signature updates) and set general options for the display of the ZoneAlarm security software Control Center.

Setting product preferences

Use the Preferences panel to set or change your ZoneAlarm security software password, log in or log out, manage product feature updates (but not virus signature updates), set general options for the display of the ZoneAlarm security software Control Center.

- Setting product update options
- Setting your password
- Backing up and restoring your ZoneAlarm settings
- Setting general product preferences
- Setting contact preferences
- Creating an online fraud protection profile

Setting product update options

When you purchase ZoneAlarm security software you receive a year of free updates to your product, which means you can receive the bug fixes, new features, and enhancements included in any updates to the product.

You can check for product updates manually, or set ZoneAlarm security software to check automatically.

Tip: See http://download.zonealarm.com/bin/free/information/releaseHistories.html to find out about enhancements and fixes included in any updates.

Product updates are different than virus signature updates. To control virus signature updates, which happen automatically and in the background, see "Keeping virus definitions up-to-date," on page 121.

To set product update settings:

1. Select **Overview | Preferences**.
2. In the Check for Updates area, choose an update option.

Automatically	ZoneAlarm security software automatically notifies you when an update is available. (Recommended)
Manually	You monitor the Overview panel for updates.

To invoke a product check immediately, click **Check for Update**.

Setting your password

By setting a password, you prevent anyone but you from shutting down or uninstalling ZoneAlarm security software, or changing your security settings. Setting a password will not prevent other people from accessing the Internet from your computer.

If your version of ZoneAlarm security software was installed by an administrator with an installation password, that administrator can access all functions.

When you set a password for the first time, be sure to log out before leaving your computer. Otherwise, others can still change your settings.

To set or change a ZoneAlarm security software password:

1. Select **Overview | Preferences**.
2. Click **Set Password**.
3. Type your password and password verification in the fields provided.
4. Select **Allow others to use programs without a password** (unless the program permission is set to "Block") to allow others to use programs you haven't explicitly blocked, even if they don't have a password.
5. Click **OK**.

Valid passwords are between 6 and 31 characters long. Valid characters include A-Z, a-z, 0-9, and characters !,@,#,$,%,^,&,*.

Once you have set a password, you must log in before you can change settings, shut down the TrueVector security engine, or uninstall ZoneAlarm security software.

Backing up and restoring your ZoneAlarm settings

You can back up your existing settings to an XML file so that you can restore them later or use the same settings on another computer, should you need to.

The backup and restore feature should not be used to share settings among different computers or to distribute security policies. To do so could cause an extremely high number of alerts to appear due to differences among computers, applications, and Windows processes.

To back up your ZoneAlarm security settings

1. Select **Overview**|**Preferences**.
2. In the Backup and Restore Security Settings area, click **Backup**.
3. Type a file name or select an existing file to overwrite.
4. Click **Save**.

Note that for technical support purposes a backup settings .xml file is automatically created from time to time and placed in your Internet Logs folder.

To restore your saved ZoneAlarm security settings

1. Select **Overview**|**Preferences**.
2. In the Backup and Restore Security Settings area, click **Restore**.
3. Select the XML file which contains the settings you want to use.
4. Click **Open**.

Setting general product preferences

By default, ZoneAlarm security software starts automatically when you turn on your computer. Use the settings in the General area to change this and other options.

To set general display preferences:

1. Select **Overview**|**Preferences**.

2. In the General area, specify your preferences.

Load ZoneAlarm security software at startup	ZoneAlarm security software starts automatically when you turn on your computer.

3. In the General area, click **Options**.

   The Options dialog box appears.

4. In the Display settings area, choose your display preferences.

Remember the last panel visited	Opens ZoneAlarm security software to the panel that you had open the last time you closed the Control Center.
Color-scheme	Allows you to change the default color scheme of the Control Center.

5. In the Proxy Configuration area, enter the IP address of your proxy server information only if you are certain that it is necessary to do so.

ZoneAlarm security software automatically detects most proxy configurations, such as those configured through Internet Explorer. making it unnecessary to enter that information here. You should enter proxy information only if you have an uncommon proxy configuration, such as a scripted proxy, and if some product features such as anti-virus updates or instant messaging aren't working.

Setting contact preferences

Setting contact preferences ensures that your privacy is protected when ZoneAlarm security software communicates with ZoneAlarm (for example, to check automatically for virus signature updates).

To set contact preferences:

1. Select **Overview**|**Preferences**.

2. In the Contact with ZoneAlarm area, specify your preferences.

Alert me with a pop-up before I make contact	Displays a warning before contacting ZoneAlarm to deliver registration information, get product updates, research an alert, or access DNS to look up IP addresses. **Note**: There are certain situations in which you will not be notified before contact is made. Those include sending DefenseNet data to ZoneAlarm, contacting ZoneAlarm for program advice, when an anti-virus update is performed, or when monitoring your anti-virus status. The "Share setting anonymously..." setting below, turns off the DefenseNet transfer. All other settings can be disabled from the main panel of their respective panels.

Hide my IP address when applicable	Prevents your computer from being identified when you contact ZoneAlarm, a Check Point Software Technologies, Inc. Company.
Hide the last octet of my IP address when applicable	Omits the last section of your IP address (for example, 123.456.789.XXX) when you contact ZoneAlarm, a Check Point Software Technologies, Inc. Company.
Share my security settings anonymously with ZoneAlarm	Periodically sends anonymous configuration data to ZoneAlarm. For more information, see "Joining the DefenseNet community," on page 12. **Note**: Configuration data is not collected from ZoneAlarm or ZoneAlarm Anti-virus users.

Setting product display and proxy server options

You can use the Options dialog box to specify display setting options and proxy server information.

To set product display and proxy options:

1. Select **Overview**|**Preferences**.
2. In the **General** area, click **Options**.

   The Options dialog box appears.
3. In the Display settings area, specify your preferences.

Remember the last panel visited	Opens ZoneAlarm security software to the most recently viewed panel the next time you open the Control Center.
Color-scheme	Allows you to change the default color scheme of the Control Center.

4. Enter proxy server information, where necessary.

ZoneAlarm Security Software automatically detects most proxy configurations, such as those configured through Internet Explorer, making it unnecessary to enter that information here. You only need to enter your proxy information if you have an uncommon proxy configuration, such as a scripted proxy, and if you find that some product features such as anti-virus updates aren't working.

Creating an online fraud protection profile

If you are an eBay user, you can protect yourself against online fraud by storing your online credentials in ZoneAlarm security software. ZoneAlarm security software protects your profile by making sure it is only sent to authorized eBay destinations.

To create your online protection profile in ZoneAlarm and ZoneAlarm Anti-virus:

1. Select **Overview**|**Preferences**.

2. In the eBay Protection Profile area, click **Password**.

   The Alliance Partner Password dialog displays.

3. Select eBay from the Alliance Partner drop-down list.

4. Type your eBay password into the password and confirm fields, then click **OK**.

To enter your eBay password:

1. Select **ID Lock|myVAULT**, then click **Add**.

   The Add information to myVAULT dialog appears.

2. Type a description of the item, then select **eBay password** from the category drop-down list.

3. Type your eBay password into the password and confirm fields, then click **OK**.

   Asterisks will appear in place of the data you entered and an encrypted form of your eBay password will be stored in myVAULT. The original information is not stored on your computer.

4. Specify whether you want the information to be protected when using Web and E-mail.

5. Click **OK** to save your changes.

   For more information about how ZoneAlarm security software keeps passwords and other personal data safe, see Chapter 10,"Identity protection," starting on page 160.

Licensing, registration, and support

In order to receive support and updates for ZoneAlarm security software, you need a valid license.

- When your license expires
- Renewing your product license
- Updating your ZoneAlarm registration information
- Accessing technical support

When your license expires

When you purchase a ZoneAlarm product, it is yours to use forever. With the purchase you also receive one or more years of online technical support and free updates to your version of the software. These updates include product updates as well as anti-virus/antispyware signature updates, to keep you protected from new malware as it is discovered.

Once the license expires, you can renew it to receive product updates and technical support. If you do not renew your license, the product continues to work as it has been, but is not updated to detect newly discovered malware.

To find out if your license key is still valid, click **Overview** | **Product Info** | **Change Lic**. Your license key expiration date and time appear directly underneath the license number.

Renewing your product license

When your license or trial expires, you will see messages that provide a button for renewal. Or, you can renew by following the instructions below.

To renew a license:

1. Select **Overview**|**Product Info**.
2. In the Licensing Information area, click **Renew.**

You will be directed to a ZoneAlarm Web page where you can complete renewal.

Important: After you renew your license or enter a new license, click the **Check for Updates** link on in the ZoneAlarm window. This completes your renewal.

If you need help finding your license key, or have any other problems with your license key, please refer to http://www.zonealarm.com/support for assistance and answers to common questions.

When you upgrade to a product with more features, the installation wizard helps you preserve your previous ZoneAlarm security software settings if possible. In case it is not possible, it's a good idea to save your settings by using the **Overview** | **Preferences** | **Backup** function before upgrading. After upgrading, use the **Overview** | **Preferences** | **Restore** function to import your settings.

If you have been using a trial or beta license key and have just purchased a full license, you can enter the license key in the following manner.

To change your license key:

1. Under **Quick Tasks**, click **Enter License Key**.
2. In the dialog that appears, either type or *copy and paste* your license key, then click **OK**.

Accessing technical support

From **Overview** panel, you can access to support resources, such as Frequently Ask Questions, known issues, and how to contact support.

To access support resources:

1. Select **Overview**|**Product Info**.

2. In the Support and Update Information area, click the **click here** link.

   The Support Center Web site appears.

Updating your ZoneAlarm registration information

When you purchase ZoneAlarm security software, you are registered and can receive security news from ZoneAlarm. If your information changes, you can update it.

To update your registration information:

1. Select **Overview**|**Product Info**.
2. In the Registration area, click **Change Reg**.
3. Enter your information in the fields provided.

   To be notified of product news and updates, select the check box labeled **Inform me of important updates and news**, then click **OK**.

Updating and upgrading your product

About updating from a prior version

When you purchase ZoneAlarm security software, you receive automatic product updates for the length of the license you purchased, which means that when a new version of your ZoneAlarm security software is released, your software notifies you and you can download it instantly for free. You can also get the latest version by doing the following:

1. Open ZoneAlarm.
2. Click **Overview** | **Preferences**
3. Click the **Check for Update** button.

When you update from a prior version, the installer program preserves your ZoneAlarm settings when possible. In some cases, the installer may determine that you need to perform Clean installation, which will not preserve your settings. However, you can save your settings in either case by using the **Overview** | **Preferences** | **Backup** function before updating. After updating, use the **Overview** | **Preferences** | **Restore** function to import the .xml settings file you saved.

Upgrading to another ZoneAlarm product

To find out how you can upgrade to more features:

1. Open ZoneAlarm.

2. Click the "Verify you are running all necessary protection on this computer" link in the lower middle of the window.

   A window opens to guide you through product upgrade options.

When upgrading to a new product with more features, it's a good idea to save your settings beforehand by using the **Overview** | **Preferences** | **Backup** function. After upgrading, use the **Overview** | **Preferences** | **Restore** function to import the .xml settings file you saved.

Uninstalling ZoneAlarm

To uninstall your ZoneAlarm product:

1. From the Windows **Start** menu, choose **All Programs | ZoneAlarm | Uninstall ZoneAlarm Security**.
2. Click the **Uninstall** button in the dialog that appears, and follow the onscreen instructions.

Moving to a different computer

If you wish to move ZoneAlarm to a new machine, per the licensing agreement, completely remove it from the existing machine, and then install it on the new machine. Use the same license key that you used previously.

If you have a multi-user license, download a free trial version on each machine (from http://www.zonealarm.com) or use your CD and the same license key on each machine. Enter your ZoneAlarm license key on the new computer by clicking **Enter License Key** under **Quick Tasks** in the ZoneAlarm window.

Chapter 2

Configuring for networks and resources

If you're on a home network, business Local Area Network (LAN), or Virtual Private Network (VPN), or a wireless network, you want to ensure smooth communication with the network while still maintaining high security. The Network Configuration Wizard, automatic VPN configuration, and other features of ZoneAlarm security software help you to quickly set up your network environment.

Topics:

- "Configuring a new network connection," on page 23
- "Integrating with network services," on page 26
- "Configuring your VPN connection," on page 27

Configuring a new network connection

If your computer connects to a network, you have to decide whether to place that network in the Trusted Zone or in the Internet Zone.

Placing a network in the Trusted Zone enables you to share files, printers, and other resources with other computers on that network. Networks you know and trust, such as your home or business LAN and known protected wireless networks, should go in the Trusted Zone.

Placing a network in the Internet Zone prevents you from sharing resources with other computers on that network and protects you from the security risks associated with

resource sharing. Unknown networks and most wireless networks, even secured wireless networks, should go in the Internet Zone.

The Network Configuration Wizard helps you make this decision by determining whether the detected LAN network is public or private. The Wireless Network Configuration Wizard helps you make this decision by determining whether the detected wireless network is secured or unsecured.

- Using the Network Configuration Wizard
- Using the Wireless Network Configuration Wizard
- Disabling the Wireless Network Configuration Wizard

Using the Network Configuration Wizard

When your computer connects to a new network, ZoneAlarm security software opens the Network Configuration Wizard, displaying the IP address of the detected network.

The IP address of the network is used to determine whether it is a *private network* or a *public network*.

A private network is usually a home or business Local Area Network (LAN). Private networks are placed in the *Trusted Zone* by default.

A public network is usually a much larger network, such as that associated with an ISP. Public networks are placed in the *Internet Zone* by default.

To configure your network connection using the Network Configuration Wizard:

1. Choose the Zone you want this network in, then click **Next**.
2. Name the network. The name you enter here will be displayed in the Zones | Inbound Firewall panel.

If you prefer not to use the Network Configuration Wizard, click Cancel in the Wizard screen. A New Network alert will appear. The detected network will be placed in the Internet Zone, even if it is a private network. For information on using the New Network alert, see "New Network alerts," on page 83.

Disabling the Network Configuration Wizard

The Network Configuration Wizard is enabled by default. If you prefer to use the New Network Alert to configure new networks, you can disable the Network Configuration Wizard.

To disable the Network Configuration Wizard:

In screen four of the Wizard, select the check box labeled **Do not show this Wizard the next time a new network is detected,** then click **Finish**.

Using the Wireless Network Configuration Wizard

When your computer connects to a new wireless network, ZoneAlarm security software opens the Wireless Network Configuration Wizard, then displays the IP address of the detected network.

The WPA setting on the wireless access point is used to determine whether it is a *secured* wireless network or an *unsecured* wireless network.

A secured wireless network is WPA enabled. WPA provides an initial barrier that can be penetrated by hackers. In order to truly secure the network, the wireless access point must have other features implemented, such as a limited access list or SSID (Service Set Identifier) broadcast disabled. Only place wireless networks that you know have a higher level of security and where you need to share resources or print in the *Trusted Zone*.

An unsecured wireless network may be completely unprotected and accessible by anyone. Unsecured networks are placed in the *Internet Zone* by default.

To configure a wireless connection:

1. Choose the Zone you want this network in, then click **Next**.
2. Name the network.

   The name you enter in the Configuration Wizard displays on the Zones | Inbound Firewall panel.

If you prefer not to use the Network Configuration Wizard, click Cancel in any Wizard screen. A New Network alert will appear. The detected network will be placed in the Internet Zone, even if it is a secured wireless network. For information on using the New Network alert, see "New Network alerts," on page 83.

Disabling the Wireless Network Configuration Wizard

The Network Configuration Wizard is enabled by default. If you prefer to use the New Network Alert to configure new networks, you can disable the Network Configuration Wizard.

To disable the Wireless Network Configuration Wizard:

In screen four of the Wizard, select the check box labeled **Do not show this Wizard the next time a new network is detected,** then click **Finish**.

Integrating with network services

If you're working on a home or business network, you may want to share files, network printers, or other resources with other people on the network, or send and receive e-mail through your network's mail servers. Use the instructions in this section to enable safe resource sharing.

- Enabling file and printer sharing
- Connecting to network mail servers
- Enabling Internet Connection Sharing

Enabling file and printer sharing

To share printers and files with other computers on your network, you will need to configure ZoneAlarm security software to allow access to the computers with which you plan to share resources.

To configure ZoneAlarm security software for file and printer sharing:

Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone:

- Go to the **Firewall** | **Zones** panel.
- Under the **Name** column, find your home network (it may be the only listing), and on that row right-click the word "Internet" under **Zone** and choose **Trusted** from the pop-up menu.

If the default Trusted Zone security level has been changed, reset it to Medium. This allows trusted computers to access your shared files.

If the default Internet Zone security level has been changed, reset it to High. This makes your computer invisible to non-trusted machines.

See "Setting the security level for a Zone," on page 34.

Connecting to network mail servers

ZoneAlarm security software is configured to automatically work with Internet-based mail servers using POP3 and IMAP4 protocols, when you give your e-mail client permission to access the Internet.

Some mail servers, like Microsoft Exchange, include collaboration and synchronization features that might require you to trust the server in order for those services to work.

To configure ZoneAlarm security software for mail servers with collaboration and synchronization features:

1. Add the network subnet or IP address of the mail server to your Trusted Zone.
2. Set the Trusted Zone security level to Medium. This allows server collaboration features to work.
3. Set Internet Zone security level to High. This makes your computer invisible to non-trusted machines.

Enabling Internet Connection Sharing

If you are using Windows' Internet Connection Sharing (ICS) option, or a third-party connection sharing program, you can protect all of the computers that share the connection from inbound threats by installing ZoneAlarm security software on the gateway machine only. However, to receive outbound protection, or to see alerts on the client machines, you must have ZoneAlarm security software installed on the client machines as well.

Before you configure ZoneAlarm security software, use your ICS software to set up the gateway and client relationships. If you use hardware such as a router to share your Internet connection rather than Microsoft's Internet Connection Sharing (ICS), ensure that the local subnet is in the Trusted Zone.

Configuring your VPN connection

ZoneAlarm security software is compatible with many types of VPN client software and can automatically configure the connection for certain VPN clients.

- Supported VPN protocols
- Configuring your VPN connection automatically
- Configuring your VPN connection manually
- Adding a VPN gateway and other resources to the Trusted Zone
- Removing a VPN gateway from a blocked range or subnet

- Allowing VPN protocols
- Granting access permission to VPN software

Supported VPN protocols

ZoneAlarm security software monitors the VPN protocols listed in the table below.

Networking Protocol	Explanation and Comments
AH	Authentication Header Protocol
ESP	Encapsulating Security Payload protocol
GRE	Generic Routing Encapsulation protocol
IKE	Internet Key Exchange protocol
IPSec	IP Security protocol.
L2TP	Layer 2 Tunneling protocol. L2TP is a more secure variation of PPTP.
LDAP	Lightweight Directory Access protocol
PPTP	Point-to-Point Tunneling protocol
SKIP	Simple Key Management for Internet Protocol

Table 2-1: Supported VPN protocols

Configuring your VPN connection automatically

When VPN traffic is detected, an Automatic VPN Configuration alert is displayed. Depending upon the type of VPN activity detected, and whether ZoneAlarm security software was able to configure your VPN connection automatically, you may see one of three Automatic VPN Configuration alerts.

For detailed information about the types of Automatic VPN Configuration alerts you may see and how to respond to them, see "Automatic VPN Configuration alert," on page 74.

For instance, manual action may be required if the loopback adaptor or the IP address of the VPN gateway falls within a range or subnet that you have blocked. For more information, see "Configuring your VPN connection manually," on page 29.

If you have created an expert firewall rule that blocks VPN traffic, you will need to modify the expert rule to allow VPN traffic. See "Creating expert firewall rules," on page 48.

Configuring your VPN connection manually

If your VPN connection cannot be configured automatically, ZoneAlarm security software displays a Manual Action Required alert informing you of the manual changes you need to make to configure your connection.

Refer to the following sections for manual configuration instructions:

- Adding a VPN gateway and other resources to the Trusted Zone
- Removing a VPN gateway from a blocked range or subnet
- Allowing VPN protocols
- Granting access permission to VPN software

If you have created an expert firewall rule that has blocked PPTP traffic and your VPN software uses PPTP, you will need to modify the expert rule. See “Creating expert firewall rules,” on page 48.

Adding a VPN gateway and other resources to the Trusted Zone

In addition to the VPN gateway, There may be other VPN-related resources that need to be in the Trusted Zone for your VPN to function properly.

Required Resources	Other Resources
The resources below are required by all VPN client computers and must be added to the Trusted Zone.	The resources below may or may not be required, depending on your specific VPN implementation.
VPN Concentrator	DNS servers
Remote host computers connected to the VPN client (if not included in the subnet definitions for the corporate network)	Local host computer's NIC loopback address (depending on Windows version). If you specify a local host loopback address of 127.0.0.1, do not run proxy software on the local host.
Corporate Wide Area Network (WAN) subnets that will be accessed by the VPN client computer	Internet Gateway
Corporate LANs that will be accessed by the VPN computer	Local subnets
	Security servers (for example, RADIUS,ACE, or TACACS servers)

Table 2-2: Required VPN-related network resources

See "Adding to the Trusted Zone," on page 40, to learn how to add resources to your computer's Trusted Zone.

Removing a VPN gateway from a blocked range or subnet

If the VPN gateway falls within a range or subnet that you have blocked, you must manually unblock the range.

To unblock an IP range or subnet:

1. Select **Firewall**|**Zones.**
2. In the Zone column, select the blocked IP range or subnet.
3. Select **Trusted** from the shortcut menu, then click **Apply**.

Allowing VPN protocols

To ensure proper configuration of your VPN software with ZoneAlarm security software, you will need to modify your general security settings to allow VPN protocols.

To allow VPN protocols:

1. Select **Firewall** |**Advanced**.

2. In the General settings area, select the check box labeled **Allow VPN protocols**.
3. Click **OK**.

If your VPN program uses protocols other than GRE, ESP, and AH, also select the check box labeled **Allow uncommon protocols at high security**.

Granting access permission to VPN software

Grant access permission to the VPN client and any other VPN-related programs.

To grant permission to your VPN program:

1. Select **Program Control**|**Programs**.
2. In the Programs column, select your VPN program.
3. In the Access column, click below Trusted, then select **Allow** from the shortcut menu.

If your VPN program is not listed, click **Add** to add it to the list.

To grant access to VPN-related components:

1. Select **Program Control**|**Components**.
2. In the Components column, select the VPN component for which you want to grant access.
3. In the Access column, select **Allow** from the shortcut menu.

If you are experiencing problems with your VPN connection, refer to the VPN troubleshooting tips in Appendix 14,"Troubleshooting," starting on page 197.

Chapter 3

Firewall protection

Firewall protection is your front line of defense against Internet threats. ZoneAlarm security software's default Zones and security levels give you immediate protection against the vast majority of threats. If you're an advanced user, custom port permissions and expert rules give you detailed control of traffic based on source, destination, port, protocol, and other factors.

Topics:

- "Understanding Firewall protection," on page 33
- "Choosing security levels," on page 34
- "Setting advanced security options," on page 35
- "Managing traffic sources," on page 39
- "Blocking and unblocking ports," on page 43
- "Understanding expert firewall rules," on page 46
- "Creating expert firewall rules," on page 48
- "Creating groups," on page 50
- "Managing Expert Firewall Rules," on page 54

Understanding Firewall protection

In buildings, a firewall is a barrier that prevents a fire from spreading. In computers, the concept is similar. There are a variety of "fires" out there on the Internet—hacker activity,

viruses, worms, and so forth. A firewall is a system that stops these attempts to damage your computer.

The ZoneAlarm security software firewall guards the "doors" to your computer—that is, the ports through which Internet traffic comes in and goes out. ZoneAlarm security software examines all the network traffic arriving at your computer, and asks these questions:

- What Zone did the traffic come from and what port is it addressed to?
- Do the rules for that Zone allow traffic through that port?
- Does the traffic violate any global rules?
- Is the traffic authorized by a program on your computer (Program Control settings)?

The answers to these questions determine whether the traffic is allowed or blocked.

- Choosing security levels
- Setting advanced security options
- Managing traffic sources
- Blocking and unblocking ports
- Understanding expert firewall rules

Choosing security levels

The default firewall *security levels* (High for the Internet Zone, Med. for the Trusted Zone) protect you from hacker activity (such as a *port scan*), while enabling you to share printers, files, and other resources with trusted computers on your local network. In most cases, you don't have to make any adjustment to these defaults. You're protected as soon as ZoneAlarm security software is installed!

- Setting the security level for a Zone
- Setting advanced security options

Setting the security level for a Zone

Security levels make it easy to configure your firewall settings. You can apply a preconfigured security level (High, Medium, or Off) to each Zone, or you can specify the port and protocol restrictions for each level. See "Blocking and unblocking ports," on page 43.

To set the security level for a Zone:

1. Select **Firewall**.

2. In the Internet Zone Security area, click the slider and drag it to the desired setting.

High	Your computer is in stealth mode, making it invisible to other computers. Access to Windows *NetBIOS (Network Basic Input/Output System)* services, file and printer shares **is blocked**. Ports are blocked unless you have provided permission for a program to use them.
Med	Your computer is visible to other computers. Access to Windows services, file and printer shares **is allowed**. Program permissions are still enforced.
Off	Your computer is visible to other computers. Access to Windows services, file and printer shares **is allowed**. Program permissions are still enforced.

3. In the Trusted Zone Security area, click the slider and drag it to the desired area.

High	Your computer is in stealth mode, making it invisible to other computers. Access to Windows (NetBIOS) services, file and printer shares **is blocked**. Ports are blocked unless you have provided permission for a program to use them.
Med	Your computer is visible to other computers. Access to Windows services, file and printer shares **is allowed**. Program permissions are still enforced.
Off	Your computer is visible to other computers. Access to Windows services, file and printer shares **is allowed**. Program permissions are still enforced.

Setting advanced security options

Advanced security options enable you to configure the firewall for a variety of special situations, such as gateway enforcement and Internet Connection Sharing (ICS).

- Setting gateway security options
- Setting ICS (Internet Connection Sharing) options
- Setting general security options
- Setting network security options

Setting gateway security options

Some companies require their employees to use ZoneAlarm security software when connecting to the Internet through their corporate *game mode*. When the **Automatically check the gateway**... control is selected, ZoneAlarm security software checks for any compatible gateways and confirms that it is installed so that gateways requiring ZoneAlarm security software will grant access.

You can leave this option selected even if you are not connecting through a gateway. Your Internet functions will not be affected.

Setting ICS (Internet Connection Sharing) options

If you are using *ICS (Internet Connection Sharing)*, use these controls to configure ZoneAlarm security software to recognize the ICS gateway and clients.

To set Internet Connection Sharing preferences:

1. Select **Firewall**.
2. Click **Advanced**.
3. In the Internet Connection Sharing area, choose your security settings.

This computer is not on an ICS/NAT network	Internet Connection sharing is disabled.
This is a client of an ICS/NAT gateway running ZoneAlarm security software	ZoneAlarm security software automatically detects the IP address of the ICS gateway and displays it in the Gateway Address field. You also can type the IP address into the Gateway address field. Selecting **Forward alerts from gateway to this computer** will log and display alerts on the client computer that occur on the gateway.
This computer is an ICS/NAT gateway	ZoneAlarm security software automatically detects the IP address of the ICS gateway and displays it in the Local Address field. You also can type the IP address into the Gateway address field. Selecting **Suppress alerts locally if forwarded to clients**, will suppress alerts forwarded from the gateway to clients to also be displayed on the gateway.

4. Click **OK**.

Setting general security options

These controls apply global rules regarding certain protocols, packet types and other forms of traffic (such as server traffic) to both the Trusted Zone and the Internet Zone.

To modify general security settings:

1. Select **Firewall**.
2. Click **Advanced**.
3. In the General area, choose your security settings.

Block all fragments	Blocks all incomplete (fragmented) IP data packets. Hackers sometimes create fragmented packets to bypass or disrupt network devices that read packet headers. **Caution**: If you select this option, ZoneAlarm security software will silently block all fragmented packets without alerting you or creating a log entry. Do not select this option unless you are aware of how your online connection handles fragmented packets.
Block trusted servers	Prevents all programs on your computer from acting as servers to the Trusted Zone. Note that this setting overrides permissions granted in the Programs panel.
Block Internet servers	Prevents all programs on your computer from acting as servers to the Internet Zone. Note that this setting overrides permissions granted in the Programs panel.
Enable ARP protection	Blocks all incoming ARP (Address Resolution Protocol) requests except broadcast requests for the address of the target computer. Also blocks all incoming ARP replies except those in response to outgoing ARP requests.
Allow VPN Protocols	Allows the use of VPN protocols (ESP, AH, GRE, SKIP) even when High security is applied. With this option disabled, these protocols are allowed only at Medium security.
Allow uncommon protocols at high security	Allows the use of protocols other than ESP, AH, GRE, and SKIP, at High security.
Lock hosts file	Prevents your computer's hosts file from being modified by hackers through sprayer or Trojan horses. Because some legitimate programs need to modify your hosts file in order to function, this option is turned off by default.
Disable Windows Firewall	Detects and disables Windows Firewall. This option will only appear if you are using Windows XP with Service Pack 2.
Filter IP over *1394* traffic	Filters FireWire traffic. You will need to restart your PC for these filter changes to take effect.

Click **OK**.

ZoneAlarm filters Internet Protocol version 6 (IPv6) traffic by default. When the ZoneAlarm firewall is set to block IPv6, it also tells Windows not to use it, so you will see IPv6 disabled in your network settings.

Setting network security options

Automatic network detection helps you configure your Trusted Zone easily so that traditional local network activities such as file and printer sharing aren't interrupted. ZoneAlarm security software detects only networks that you are physically connected to. Routed or virtual network connections are not detected.

You can have ZoneAlarm security software silently include every detected network in the Trusted Zone; or ask you in each case whether to add a newly detected network.

To specify Network settings:

1. Select **Firewall**.
2. Click **Advanced**.
3. In the Network settings area, choose your security settings.

Include networks in the Trusted Zone upon detection	Automatically moves new networks into the Trusted Zone. This setting provides the least security.
Exclude networks from the Trusted Zone upon detection	Automatically blocks new networks from being added to the Trusted Zone and places them in the Internet Zone. This setting provides the most security.
Ask which Zone to place new networks in upon detection	ZoneAlarm security software displays a New Network alert or the Network Configuration Wizard, which give you the opportunity to specify the Zone.
Automatically put new unprotected wireless networks (WEP or WPA} in the Internet Zone	Puts unsecured wireless networks into the Internet Zone automatically, which prevents unauthorized access to your data from others accessing the network.

4. Click **OK**.

For more information about networking, see Chapter 2,"Configuring for networks and resources," starting on page 23.

Setting wireless network security options

Automatic wireless network detection helps you configure your Internet Zone to ensure that you computer remains secure without being interrupted each time a new wireless network is detected. ZoneAlarm security software detects only wireless networks that your computer is connected to. (Networks that you are not actually connected to may appear as available networks in your network neighborhood but the New Wireless Network Configuration Wizard only appears when you connect establish a connection to that network.)

You can have ZoneAlarm security software silently include every detected wireless network in the Internet Zone.

To specify Network settings:

1. Select **Firewall**.
2. Click **Advanced**.
3. In the Wireless Network settings area, choose your security settings.

Automatically put new unprotected wireless networks (WEP or WPA) in the Internet Zone	ZoneAlarm security software places new wireless networks in the Internet Zone when they are detected.

4. Click **OK**.

For more information about networking, see Chapter 2,"Configuring for networks and resources," starting on page 23.

Managing traffic sources

The Zones panel contains the traffic sources (computers, networks, or sites) you have added to the Trusted Zone or Blocked Zone. It also contains any networks that ZoneAlarm security software has detected. If you are using a single, non-networked PC, the traffic source list displays only your ISP's (Internet Service Provider's) network, which should be in the Internet Zone.

- Viewing the traffic source list
- Modifying traffic sources
- Adding to the Trusted Zone
- Adding to the Blocked Zone
- Viewing logged Firewall events

Viewing the traffic source list

The traffic source list displays the traffic sources and the Zones they belong to. You can sort the list by any field by clicking the column header. The arrow (^) next to the header name indicates the sort order. Click the same header again to reverse the sort order.

Field	Description
Name	The name you assigned to this computer, site, or network
IP Address/Site	The IP address or host name of the traffic source

Table 3-1: Traffic source list fields

Field	Description
Entry Type	The type of traffic source: Network, Host, IP, Site, or Subnet
Zone	The Zone the traffic source is assigned to: Internet, Trusted, or Blocked

Table 3-1: Traffic source list fields

Modifying traffic sources

From the traffic source list, you can move the traffic source from one Zone to another, add, edit, or remove a traffic source.

To change the Zone of a traffic source:

1. Select **Firewall**|**Zones**.
2. Locate the traffic source, then click in the **Zone** column.
3. Select a Zone from the shortcut menu, then click **Apply**.

To add, remove, or edit a traffic source:

1. Select **Firewall**|**Zones**.
2. In the Name column, click the traffic source, then click **Add**, **Edit**, or **Remove**.
3. Click **Apply**.

Adding to the Trusted Zone

The Trusted Zone contains computers you trust want to share resources with. For example, if you have three home PCs that are linked together in an Ethernet network, you can put each individual computer or the entire network adapter subnet in the Trusted Zone. The Trusted Zone's default medium security settings enable you to safely share files, printers, and other resources over the home network. Hackers are confined to the Internet Zone, where high security settings keep you safe.

Tip: The easiest way to add something to the Trusted Zone is to go to Alerts & Logs | Log Viewer, see if the IP address, network, host, or site has shown up in the logs. Right-click it and choose **Add to Zone > Trusted**.

To add a single IP address:

1. Select **Firewall**|**Zones**.
2. Click **Add**, then select **IP address** from the shortcut menu.

   The Add IP Address dialog appears.
3. Select **Trusted** from the Zone drop-down list.
4. Type the IP address and a description in the boxes provided, then click **OK.**

To add an IP range:

1. Select **Firewall**|**Zones**.
2. Click **Add**, then select **IP address** from the shortcut menu.

   The Add IP Range dialog appears.
3. Select **Trusted** from the Zone drop-down list.
4. Type the beginning IP address in the first field, and the ending IP address in the second field.
5. Type a description in the field provided, then click **OK**.

To add a subnet:

1. Select **Firewall**|**Zones**.
2. Click **Add**, then select **Subnet** from the shortcut menu.

   The Add Subnet dialog appears.
3. Select **Trusted** from the Zone drop-down list.
4. Type the IP address in the first field, and the Subnet mask in the second field.
5. Type a description in the field provided, then click **OK**.

To add to a Host or Site to the trusted Zone:

1. Select **Firewall**|**Zones**.
2. Click **Add**, then select **Host/Site**.

   The Add Host/Site dialog appears.
3. Select **Trusted** from the Zones drop-down list.
4. Type the fully qualified host name in the **Host name** field.
5. Type a description of the host/site, then click **OK**.

To add a network to the Trusted Zone:

1. Select **Firewall**|**Zones**.
2. In the Zone column, click the row containing the network, then select **Trusted** from the shortcut menu.
3. Click **Apply**.

ZoneAlarm security software automatically detects new network connections and helps you add them to the right Zone. For more information, see Chapter 2,"Configuring for networks and resources," starting on page 23.

Adding to the Blocked Zone

To add to the Blocked Zone, follow the instructions for adding to the Trusted Zone, but select **Blocked** from the drop-down list in step 2.

Viewing logged Firewall events

By default, all Firewall events are recorded in the Log Viewer.

To view logged firewall events:

1. Select **Alerts & Logs | Log Viewer**.
2. Select **Firewall**, from the Alert Type drop-down list.

Table 5-2 provides an explanation the log viewer fields available for Firewall events.

Field	Information
Rating	Each alert is high-rated or medium-rated. High-rated alerts are those likely to have been caused by hacker activity. Medium-rated alerts are likely to have been caused by unwanted but harmless network traffic.
Date/Time	The date and time the alert occurred.
Type	The type of alert: Firewall, Program, ID Lock, or Lock Enabled.
Protocol	The communications protocol used by the traffic that caused the alert.
Program	The name of the program attempting to send or receive data. (Applies only to Program and ID Lock alerts).
Source IP	The IP address of the computer that sent the traffic that ZoneAlarm security software blocked.
Destination IP	The address of the computer the blocked traffic was sent to.
Direction	The direction of the blocked traffic. “Incoming” means the traffic was sent to your computer. “Outgoing” means the traffic was sent from your computer.
Action Taken	How the traffic was handled by ZoneAlarm security software.
Count	The number of times an alert of the same type, with the same source, destination, and protocol, occurred during a single session.
Source DNS	The domain name of the sender of the traffic that caused the alert.

Table 3-2: Firewall event log fields

Field	Information
Destination DNS	The domain name of the intended addressee of the traffic that caused the alert.

Table 3-2: Firewall event log fields

Blocking and unblocking ports

ZoneAlarm security software's default security levels determine which ports and protocols are allowed and which are blocked. If you are an advanced user, you can change the definition of the security levels by changing port permissions and adding custom ports.

- Default port permission settings
- Adding custom ports

Default port permission settings

The default configuration for High security blocks all inbound and outbound traffic through ports not being used by programs you have given access or server permission except:

- DHCP broadcast/multicast
- Outgoing DHCP (port 67) - on Windows 9x systems
- Outgoing DNS (port 53) - If the computer is configured as an ICS gateway

Traffic Type	Security levels		
	HIGH	MED	OFF
DNS outgoing	block	n/a	allow
DHCP outgoing	block	n/a	allow
broadcast/multicast	allow	allow	allow
ICMP			
incoming (ping echo)	block	allow	allow
incoming (other)	block	allow	allow
outgoing (ping echo)	block	allow	allow
outgoing (other)	block	allow	allow
IGMP			

Table 3-3: Default access permissions for incoming and outgoing traffic types

Traffic Type	Security levels		
	HIGH	MED	OFF
incoming	block	allow	allow
outgoing	block	allow	allow
NetBIOS			
incoming	n/a	block	allow
outgoing	n/a	allow	allow
UDP (ports not in use by a permitted program)			
incoming	block	allow	allow
outgoing	block	allow	allow
TCP (ports not in use by a permitted program)			
incoming	block	allow	allow
outgoing	block	allow	allow

Table 3-3: Default access permissions for incoming and outgoing traffic types

To change a port's access permission:

1. Select **Firewall**.
2. In either the Internet Zone Security or the Trusted Zone Security area, click **Custom**.

   The Custom Firewall Settings dialog appears.
3. Scroll to locate High and Medium security settings.
4. To block or to allow a specific port or protocol, click the check box beside it.

Be aware that when you select a traffic type in the High security settings list, you are choosing to ALLOW that traffic type to enter your computer under High security, thus decreasing the protection of the High security level. Conversely, when you select a traffic type in the Medium security settings list, you are choosing to BLOCK that traffic type under Medium security, thus increasing the protection of the Med security level.

5. Click **Apply**, then click **OK**.

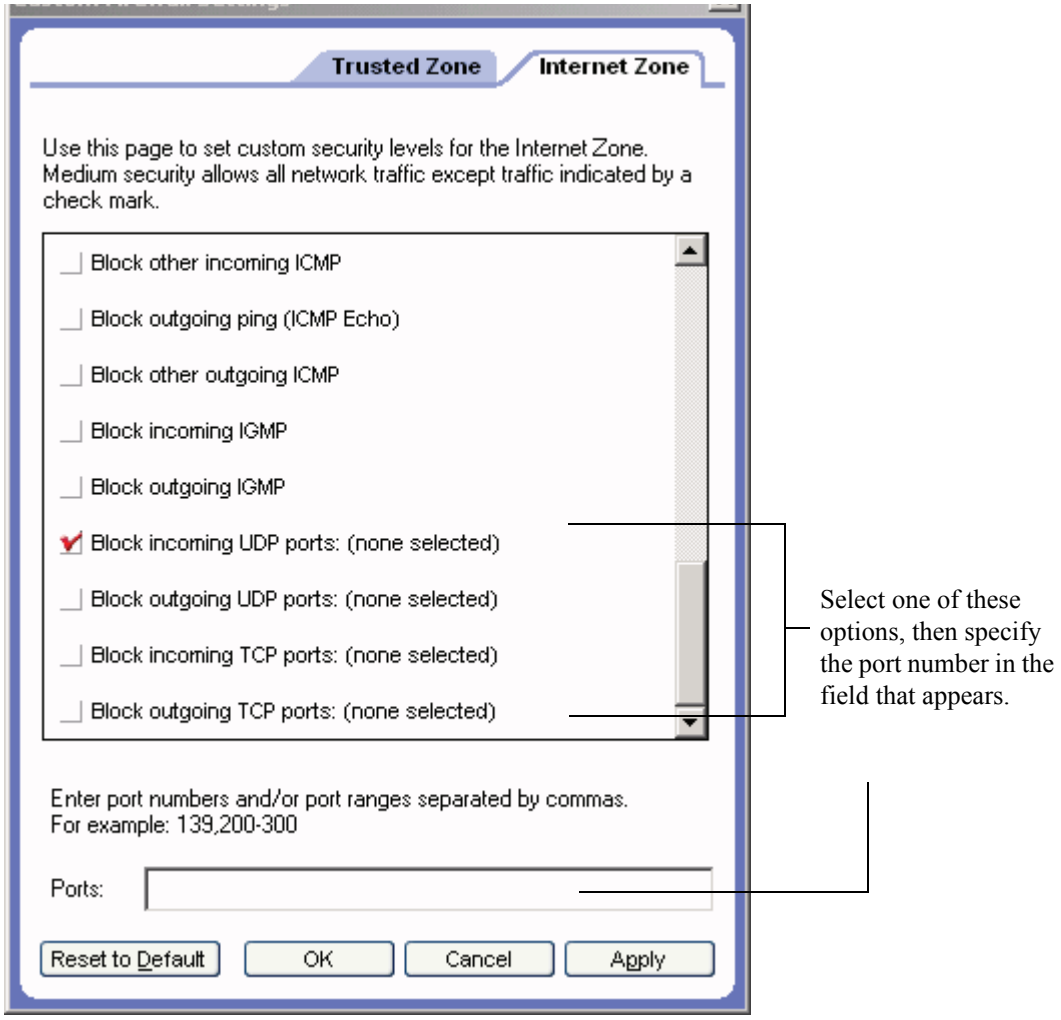
Adding custom ports

You can allow communication through additional ports at High security, or block additional ports at Medium security by specifying individual port numbers or port ranges.

To specify additional ports:

1. Select **Firewall**.
2. In either the Trusted Zone or Internet Zone area, click **Custom**.

   The Custom Firewall settings dialog appears.



3. Scroll to the security level (High or Medium) to which you want to add ports.
4. Select the desired port type: incoming UDP, outgoing UDP, incoming TCP, or outgoing TCP.
5. Type the port or port ranges you want to allow or block in the Ports field, separated by commas. For example, 139, 200-300
6. Click **Apply**, then click **OK**.

Understanding expert firewall rules

Expert firewall rules are intended for users experienced with firewall security and networking protocols.

Expert rules do not take the place of other rules. They are an integral part of the multiple layer security approach and work in addition to other firewall rules.

Expert rules use four attributes to filter packets:

- Source and/or destination IP address
- Source and/or destination port number
- Network protocol/message type
- Day and Time

Source and destination addresses can be specified in a number of formats, including a single IP network address, a range of IP addresses, a subnet description, a gateway address, or a domain name.

Source and destination ports are used only for network protocols that use ports, such as UDP and TCP/IP. ICMP and IGMP messages, for example, do not use the port information.

Network protocols can be selected from a list of common IP or VPN protocols, or specified as an IP protocol number. For ICMP, the message type can also be specified.

Day and Time ranges can be applied to a rule to restrict access based on the day of the week and the time of day.

- How expert firewall rules are enforced
- Expert firewall rule enforcement rank
- Creating expert firewall rules
- Creating groups
- Editing and re-ranking rules

How expert firewall rules are enforced

It is important to understand how expert rules are enforced in combination with Zone rules, program permissions, and other expert rules.

Expert rules and Zone rules

Expert firewall rules are enforced before Zone firewall rules. That is, if a packet matches an expert rule, that rule is enforced, and ZoneAlarm security software skips evaluation of Zone rules.

Example: Imagine you have your Trusted Zone security level set to Medium. This allows outgoing NetBIOS traffic. However, you have also created an expert rule that blocks all

NetBIOS traffic between the hours of 5PM and 7AM. Any outbound NetBIOS traffic during those hours will be blocked, in spite of the Trusted Zone setting.

Expert firewall rules and program permissions

Expert rules and Zone rules together are enforced in tandem with Program permissions. That is, if either your program permissions or Zone rules/expert firewall rules determine that traffic should be blocked, it is blocked. Note that this means that you can use firewall rules to override or redefine program permissions.

Note that packets coming from the Blocked Zone will not be blocked if they are allowed by an Expert Firewall Rule.

Expert firewall rule enforcement rank

Within the realm of firewall rules, rule evaluation order becomes a factor. ZoneAlarm security software first checks expert firewall rules. If a match is found and a rule is enforced, the communication is marked as either blocked or allowed, and ZoneAlarm security software skips evaluation of Zone rules. If no expert firewall rule is matched, ZoneAlarm security software checks Zone rules to see if the communication should be blocked.

The enforcement rank of expert firewall rules is also important. Each rule has a unique rank number, and rules are evaluated in order of rank. Only the first rule that matches is executed. Consider these two
rules:

			Name	Source	Destination	Protocol	Time	Comments
1	✓		FTP Allow	My Computer	Trusted Zone	FTP	Any	
2	✗		FTP Block	My Computer	Any	FTP	Any	

Figure 3-4: Expert firewall rule rank order

Rule 1 allows FTP clients in the Trusted Zone to connect to an FTP server on port 21. Rule 2 blocks all FTP clients from connecting on port 21, regardless of Zone. These two rules together allow clients in the Trusted Zone to use an FTP server on the client computer, but block all other FTP access.

If the order of the rules were reversed, Rule 2 would match first, and all FTP access would be blocked. Rule 1 would never have a chance to execute, so the FTP clients in the Trusted Zone would still be blocked.

Creating expert firewall rules

Creating expert firewall rules involves specifying the source or destination of the network traffic to which the rule applies, setting tracking options, and specifying the action of the rule: whether to block or to allow traffic that meets the specifications of the rule. You can create new rules from scratch, or you can copy an existing rule and modify its properties.

To create a new expert firewall rule:

1. Select **Firewall**|**Expert**, then click **Add**.

   The Add rule dialog appears.

2. In the General area, specify the rule settings.

Rank	The order in which rules will be enforced. A rule with a rank of 1 is enforced first.
Name	Provide a descriptive name for the rule.
State	Specify whether the rule is enabled or disabled.
Action	Indicates whether to block or allow traffic that matches this rule.
Track	Indicates whether to log, alert and log, or do nothing when the expert rule is enforced.
Comments	Optional field for entering notes about the expert rule.

3. In the Source area, select a location from the list, or click **Modify**, then select **Add location** from the shortcut menu. You can add any number of sources to a rule.

My Computer	Applies the expert rule to traffic originating on your computer.
Trusted Zone	Applies the expert rule to network traffic from sources in your Trusted Zone.
Internet Zone	Applies the expert rule to network traffic from sources in your Internet Zone.
All	Applies the expert rule to network traffic coming from any source.
Host/Site	Applies the expert rule to network traffic coming from specified domain name.
IP Address	Applies the expert rule to network traffic coming from specified IP address.
IP Range	Applies the expert rule to network traffic coming from a computer within the specified IP range.
Subnet	Applies the expert rule to network traffic coming from a computer within the specified subnet.
Gateway	Applies the expert rule to network traffic coming from a computer on the specified gateway.
New Group	Choose this option, then click **Add** to create a new location group to apply to the expert rule.

Existing Group	Choose this option to select one or more location groups to apply to the expert rule, then click **OK**.

4. In the Destination area, select a location from the list, or click **Modify**, then select **Add location** from the shortcut menu.

   Available location types are the same for Source and Destination locations.

5. In the Protocol area, select a protocol from the list, or click **Modify**, then select **Add Protocol**.

Add Protocol	Choose this option to add a protocol to the rule. Specify: TCP, UDP, TCP + UDP, ICMP, IGMP, or Custom and refer to Step 5 of "Creating a protocol group," on page 51 for help with this dialog.
New Group	Choose this option, then click **Add** to create a new protocol group to apply to the expert rule. See "Creating a protocol group," on page 51 for help with this dialog.
Existing Group	Choose this option to select one or more protocol groups to apply to the expert rule, then click **OK**.

6. In the Time area, select a time from the list, or click **Modify**, then select **Add Time**.

Day/Time Range	Choose this option to add a day/time range to the rule. Specify a description, time range and one or more days. Time range is specified using a 24 hour clock.
New Group	Choose this option, then click **Add** to create a new day/time group to apply to the expert rule.
Existing Group	Choose this option to select one or more day/time groups to apply to the expert rule, then click **OK**.

7. Click **OK**.

To create a new rule from an existing rule:

1. Select **Firewall**|**Expert**.
2. Select the expert firewall rule you want to duplicate, then either press **Ctrl**+**C** or right-click the rule and choose **Copy**.
3. Paste the copied rule either by pressing **Ctrl**+**V**, or by right-clicking and choosing **Paste**.

If a rule is currently selected in the list, the pasted rule will be inserted above the selected rule. If no rule is selected, the pasted rule will be inserted at the top of the rules list.

A "1" is appended to the name of the copied rule. If you paste a rule a second time, the number 2 is appended to the second rule copied.

4. Click **Apply** to save your changes.

5. Right-click the new rule and choose **Edit** to modify the rule properties as necessary.

Creating groups

Use groups to simplify the management of locations, protocols, and days/times that you use in your expert firewall rules.

- Creating a location group
- Creating a protocol group
- Creating a day/time group

Creating a location group

Use location groups to combine non-contiguous IP addresses and ranges, or different types of locations (for example, subnets and hosts), into an easily manageable set. You can then easily add that set of locations to any expert firewall rule.

Once created, the names of groups cannot be changed. For example, if you create a Location Group named "Home" and subsequently decide to call the group "Work", you would need to remove the group called "Home" and create a new group with the name "Work."

To create a location group:

1. Select **Firewall**|**Expert**, then click **Groups**.

   The Group Manager dialog appears.

2. Select **Locations**, then click **Add**.

   The Add Location Group dialog appears.

3. Specify the name and description of the location group, then click **Add** and select a Location type from the menu.

Host/Site	A description and host name of the Host/Site location, then click **OK**. Do not include http:// in the host name. Click **Lookup** to preview the site's IP address.
IP Address	A description and IP address of the IP Address location, then click **OK**.
IP Range	A description and beginning IP address and ending IP address of the IP Range location, then click **OK**.
Subnet	Specify a description, IP address, and Subnet Mask of the Subnet location, then click **OK**.

Gateway	Specify an IP address, MAC Address, and description of the Gateway location, then click **OK**.

4. Click **OK** to close the Group Manager dialog box.

Creating a protocol group

Create a protocol group to combine well-known TCP/UDP ports, protocols, and protocol-specific message types (for example, ICMP message types), into sets that you can easily add to expert rules. For example, you might create a group including POP3 and IMAP4 protocols in order to simplify the administration of your rules regarding e-mail traffic.

To create a Protocol group:

1. Select **Firewall|Expert**, then click **Groups**.

   The Group Manager dialog appears.

2. Select **Protocols**, then click **Add**.

   The Add Protocol Group dialog appears.

3. Specify the name and description of the Protocols group, then click **Add**.

   The Add Protocol dialog appears.

4. Select a protocol type from the **Protocol** drop-down list

5. Depending on the protocol type you chose, do one of the following:

   If you chose TCP, UDP, or TCP/UDP, specify a destination, source and port number.

Name	Port number
FTP	21
Telnet	23
POP3	110
NNTP	119
NetBIOS Name	137
NetBIOS Datagram	138
NetBIOS Session	139
IMAP4	143
HTTPS	443
RTSP	554
Windows Media	1755
AOL	5190
Real Networks	7070
Other	Specify port number
FTP Data	20
TFTP	69
HTTP	80
DHCP	67
DHCP Client	68
SMTP	25
DNS	53

   If you chose ICMP in step 4, specify a description, message name, and type number.

Message name	Type number
Source Quench	4
Redirect	5
Alt	6
Echo Request	8
Router Advertisement	9
Router Solicitation	10
Time Exceeded	11
Parameter Problem	12

Timestamp	13
Timestamp reply	14
Information request	15
Information reply	16
Address Mask Request	17
Address Mask Reply	18
Traceroute	30
Other	Specify type number

If you chose IGMP, specify a description, message name, and type number.

Membership Query	17
Membership Report (ver 1)	18
Cisco Trace	21
Membership Report (ver 2)	22
Leave Group (ver 2)	23
Multicast Traceroute Response	30
Multicast Traceroute	31
Membership Report (ver 3)	34
Other	Specify type number.

If you chose Custom, specify a description, protocol type, and protocol number.

RDP	27
GRE	47
ESP	50
AH	51
SKIP	57
Other	Specify protocol number.

6. Click **OK**, to close the Add Protocol dialog.

Creating a day/time group

To allow or block network traffic to or from your computer during specified periods of time, you can create a day/time group and then add it to an expert rule. For example, to block traffic coming from pop-up ad servers during business hours, you could create a group that blocks HTTP traffic coming from a specified domain during the hours of 9 AM and 5 PM, Monday through Friday.

To create a Day/Time group:

1. Select **Firewall**|**Expert**, then click **Groups**.

   The Group Manager dialog appears.

2. Select **Times**, then click **Add**.

   The Add Time Group dialog appears.

3. Specify the name and description of the Time group, then click **Add**.

   The Add Time dialog appears.

4. Specify a description of the time, then select a time and day range.

5. Click **OK**, then click **OK** to close the Group Manager.

Managing Expert Firewall Rules

From the **Firewall | Expert** panel, you can view the status of existing expert rules, enable or disable rules, edit or remove rules, add new rules, change the order of rules, and create groups.

- Understanding expert firewall rules
- Creating expert firewall rules
- Editing and re-ranking rules
- Viewing the Expert Rules list
- Editing and re-ranking rules

Viewing the Expert Rules list

The Expert Rules panel presents a list of all expert firewall rules. Rules are listed in order of enforcement priority (rank). The arrow buttons on the right-hand side more selected rules up and down the list, changing the enforcement order of the selected rules.

You also can change rank order of rules by dragging and dropping rules from one position to another.

For example, dragging and dropping rule 2 to the top of the list changes the rank of that rule to 1.

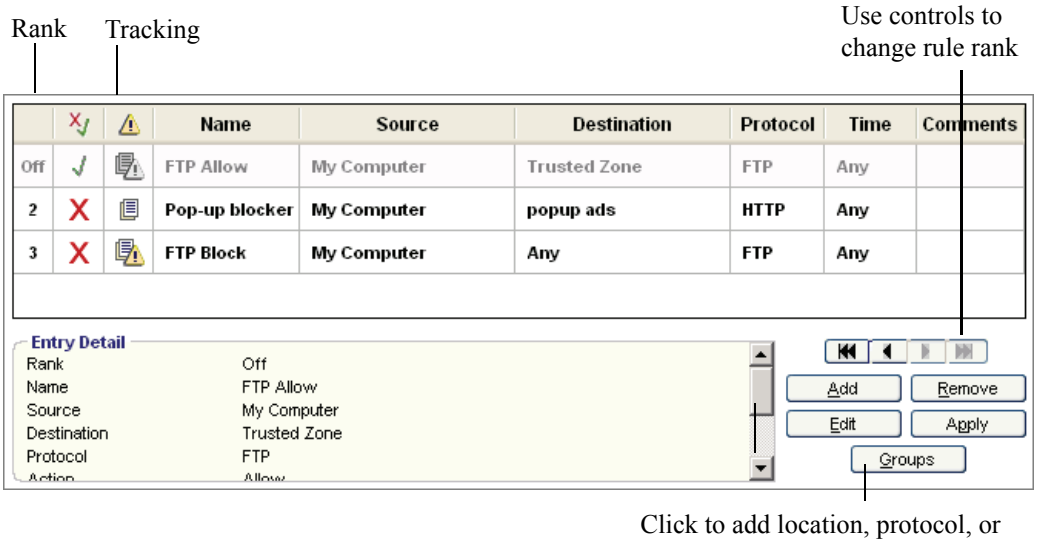


Figure 3-5: Expert Rules list

Rank

The enforcement priority of the rule. Rules are evaluated in order of rank, starting with number 1, and the first rule that matches will be enforced. Disabled rules will display "Off" instead of a rank number, but will retain their rank ordering in the list.

Action

A red X means the rule will block network traffic; a green check mark ✓ means the rule will allow network traffic.

Track

None means no notification when the rule is applied. Log ( ) means a log entry will be created when the rule is applied. Alert and Log ( ) means that an alert will be displayed and a log entry will be created when an expert rule is applied.

Name

A descriptive name for the rule.

Source

The source addresses and ports for the rule.

Destination
The destination addresses and ports for the rule.

Protocol
The network protocol to which the rule applies.

Time
The time period during which the rule is active.

Editing and re-ranking rules

You can edit or reorder existing expert rule from the Expert Rules list by selecting rules and dragging them into the desired rank. Note that if you have copied an expert rule into the rules for a Program, changing the expert rule does not automatically change the Program rule. For more information, see "Creating expert rules for programs," on page 111.

To edit a rule:

1. Select **Firewall**|**Expert**.
2. Select the rule you want to edit, then click **Edit**.

   The Edit Rule dialog appears.
3. Modify rule attributes as necessary, then click **OK**.

To change the rank of a rule:

1. Select **Firewall**|**Expert**.
2. Right-click the rule you want to move, then select **Move Rule**.

Move to Top	Moves the selected rule to the top of the Rules list.
Move to Bottom	Moves the selected rule to the bottom of the Rules list.
Move Up	Moves the selected rule one row up in the Rules list.
Move Down	Moves the selected rule one row down in the Rules list.

Chapter 4

Understanding and reducing alerts

There are many different types of security alerts that you might see while ZoneAlarm security software is protecting you. Here is where you find out why certain alerts happen, what they mean, and what to do about them. You will also find tips for reducing the number of alerts you see.

Note: For information about suppressing most alerts while playing games on your computer, see "Game Mode," on page 193.

Topics:

- "About alerts and managing them," on page 59
- "Informational alerts," on page 60
- "Program alerts," on page 65
- "OSFirewall alerts," on page 75
- "ID Lock alert," on page 82
- "New Network alerts," on page 83

About alerts and managing them

ZoneAlarm security software alerts fall into three basic categories: informational, program, and network. Additional alerts that may appear if the your version of the product includes ID Lock alerts and OSFirewall alerts.

You can specify:

- Whether you want to be alerted to all security and program events, or if you only want to be notified of events that are likely a result of hacker activity.
- Whether you want to see all alerts or only High-rated alerts. (Although some Program and ID Lock alerts cannot be suppressed as they need you to decide whether to grant permission.)

  You can also configure and monitor logs of alerts. For information about making any of these general or log settings, see "Managing Alerts and Logs," on page 181.

For details about what different types of alerts mean, how to respond to each one, and how to reduce the occurrence of each type of alert, see:

- "Informational alerts," on page 60
- "Program alerts," on page 65
- "OSFirewall alerts," on page 75
- "ID Lock alert," on page 82
- "New Network alerts," on page 83

Informational alerts

Informational alerts tell you that ZoneAlarm security software has blocked a communication that did not fit your security settings. They do not require a decision from you.

- Firewall alerts/Protected
- MailSafe alert
- Blocked Program alert
- Internet Lock alert
- Remote alert

Firewall alerts/Protected

Firewall alerts are the most common type of informational alert. Firewall alerts inform you that the ZoneAlarm security software firewall has blocked traffic based on port and protocol restrictions or other firewall rules.

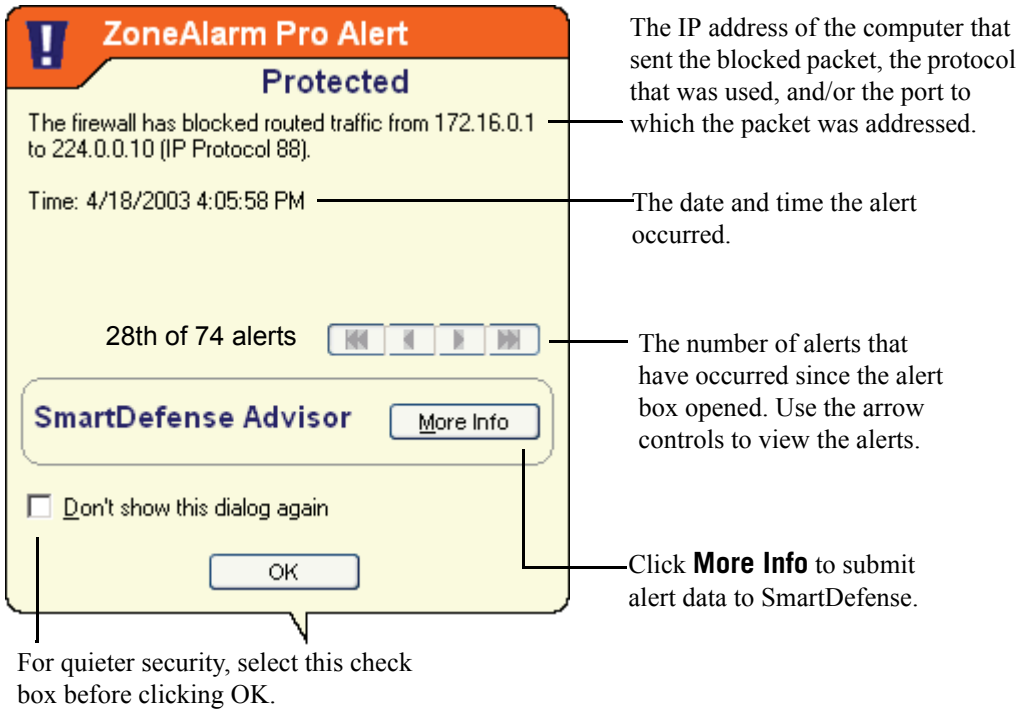


Figure 4-1: Firewall alert

Why these alerts occur

Firewall alerts with a red band at the top indicate high-rated alerts. High-rated alerts often occur as a result of hacker activity.

Firewall alerts with an orange band at the top indicate medium-rated alerts. Medium-rated alerts are likely the result of harmless network traffic, for example, if your ISP is using *ping* to verify that you're still connected. However, they also can be caused by a hacker trying to find unprotected ports on your computer.

What you should do

Informational alerts don't require a decision from you. You can close the alert by clicking **OK** at the bottom of the alert. By doing this you are not allowing any traffic to access your computer.

How to see fewer of these alerts

If you're on a home or business network, and your Trusted Zone security is set to High, normal LAN traffic such as NetBIOS broadcasts may generate firewall alerts. Try lowering Trusted Zone security to Med.

By default, ZoneAlarm security software only displays high-rated firewall alerts. If your defaults have been changed, you may see a lot of medium-rated alerts. Try setting your alert display settings to medium.

If you are receiving a large number of firewall alerts, and you are working on a home network or business LAN, it is possible that normal network communications are being blocked. If this is happening, you can eliminate the alerts by placing your network in the Trusted Zone.

Repeated alerts may indicate that a resource you want to trust is trying repeatedly to contact you. If you are receiving a lot of firewall alerts, but you don't suspect you're under attack, try the following troubleshooting steps:

- Determine if the source of the alerts should be trusted.
  - Submit repeated alerts to SmartDefense Advisor to determine the source IP address that caused the alerts.
  - If the alerts were caused by a source you want to trust, add it to the Trusted Zone.
- Determine if your Internet Service Provider is sending you "heartbeat" messages.
  - Try the procedures suggested for managing ISP heartbeat. See "Allowing ISP Heartbeat messages," on page 201.

MailSafe alert

MailSafe alerts let you know that ZoneAlarm security software has quarantined a potentially dangerous attachment to an e-mail message.

Why these alerts occur

MailSafe alerts can occur due to violations of Outbound MailSafe protection settings. A violation of Outbound MailSafe protection settings, such as an e-mail that has too many recipients, or too many e-mails within a short time, can cause a MailSafe alert to occur.

What you should do

If the alert was caused by an Outbound MailSafe violation, do the following:

- Examine the alert carefully. Does the activity noted describe actions you were recently performing? If so, you may want to modify your Outbound MailSafe settings to better accommodate your needs. See "Outbound MailSafe protection," on page 148. If not, the alert may be the result of a virus on your computer. In this case deny the outbound e-mails, then scan your computer with an anti-virus program.
- Verify that your e-mail address is listed on the approved sender's list. If you selected the **if the sender's e-mail is not in this list** option, and if your e-mail either is not on that list or is misspelled, add your valid e-mail address to the list.

How to see fewer of these alerts

Outbound MailSafe Protection is an important part of your Internet security system, and we recommend leaving it on. However, if you are getting a lot of these messages in error, you may want to adjust the sensitivity of the feature or turn it off. See "Outbound MailSafe protection," on page 148.

Blocked Program alert

Blocked Program alerts tell you that ZoneAlarm security software has prevented an application on your computer from accessing the Internet or Trusted Zone resources. By clicking OK, you're not allowing the program access, just acknowledging that you saw the alert.

Why these alerts occur

Blocked Program alerts occur when a program tries to access the Internet or the Trusted Zone, even though you have explicitly denied it permission to do so.

What you should do

If the program that was blocked is one that you want to have access to the Internet Zone or Trusted Zone, use the Programs panel to give the program access permission.

How to see fewer of these alerts

To turn off Blocked Program alerts, do either of the following:

- When you see a Blocked Program alert, select **Do not show this dialog again** before clicking **OK**. From then on, all Blocked Program alerts will be hidden. Note that this will not affect New Program, Repeat Program, or Server Program alerts.
- In the Program Control panel, click **Advanced** to access the Alerts & Functionality panel, then clear the check box labeled **Show alert when Internet access is denied**.

Turning off Blocked Program alerts does not affect your level of security.

Internet Lock alert

Internet Lock alerts let you know that ZoneAlarm security software has blocked incoming or outgoing traffic because the Internet Lock (or the Stop button) is engaged. By clicking OK, you're not opening the lock; you're just acknowledging that you've seen the alert.

If the Internet Lock has been engaged automatically (or accidentally), open it to prevent further alerts. See "Firewall zone basics," on page 10.

Why these alerts occur

These alerts occur only when the Internet Lock is engaged.

What you should do

Click **OK** to close the alert pop-up.

If the Internet Lock has been engaged automatically (or accidentally), open it to prevent further alerts. See "Firewall zone basics," on page 10.

You may want to give certain programs (for example, your browser) permission to bypass the Internet Lock, so that you can continue to perform some basic functions under the lock's higher security. See "Setting passlock permission for a program," on page 109.

How to see fewer of these alerts

If you are receiving a lot of Internet Lock alerts, it is possible that your Automatic Internet Lock settings are engaging the Internet Lock after every brief period of inactivity.

To reduce the number of alerts, you can do either of the following:

- Turn off the Automatic Internet Lock.
- Increase the interval of inactivity required to engage the Automatic Internet Lock to engage. For more information, see "Enabling the automatic lock," on page 98.

Remote alert

Remote alerts are displayed on an ICS client machine when ZoneAlarm security software blocked traffic at the ICS gateway. If you are not on a machine that is a client in an ICS network, you will never see this alert.

Why these alerts occur

Remote alerts occur when:

- ZoneAlarm security software starts up on the ICS gateway. The alert displays the message "The remote firewall has started."
- ZoneAlarm security software shuts down on the ICS gateway. The alert displays the message "The remote firewall has stopped."
- The Internet Lock has engaged on the ICS gateway. This may prevent the client machine from performing some tasks. The alert displays the message "The remote firewall has engaged the Internet Lock."
- The Internet Lock is opened on the ICS gateway. The alert displays the message "The remote firewall has disengaged the Internet Lock."

What you should do

Click **OK** to close the alert box. You do not have to do anything else to ensure your security.

How to see fewer of these alerts

If you do not want to see Remote alerts on the ICS client machine:

1. Select **Firewall**, then click **Advanced**.
2. In the Internet Connection Sharing area, clear the check box labeled **Forward alerts from gateway to this computer**.

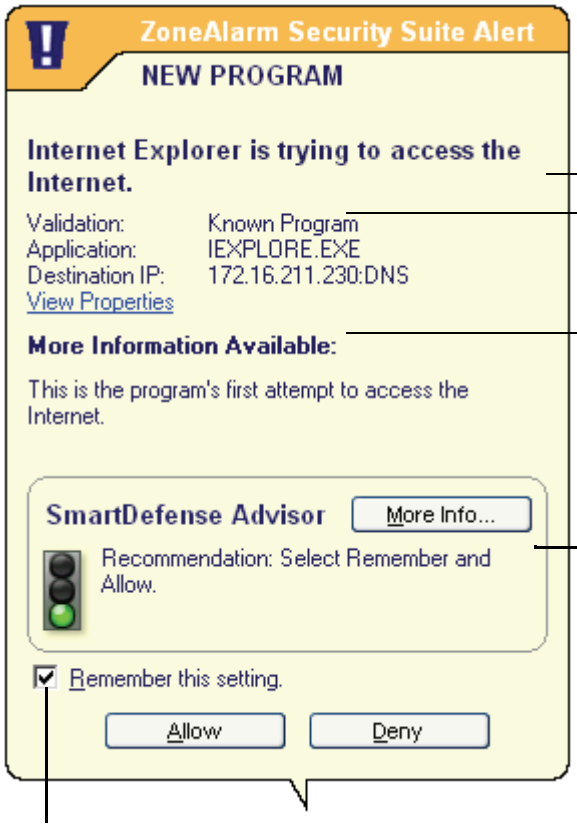
Program alerts

Program control, which generates program alerts, is the most important part of your strong outbound protection system.

Most of the time, you're likely to see program alerts when you're using a program. For example, if you've just installed ZoneAlarm security software, and you immediately open Microsoft Outlook and try to send an e-mail message, you'll get a program alert asking if you want Outlook to have Internet access. However, program alerts can also

occur if a Trojan horse or worm on your computer is trying to spread, or if a program on your computer is trying to modify your operating system.

Program alerts ask you if you want to allow a program to access the Internet or local network, or to act as a server. The most common types of Program alerts are the New Program alert and Repeat Program alert.



The name of the program that is requesting permission.

The filename of the program that requested permission, and the IP address and port number of the computer that the program is trying to contact.

When available, this area displays program advice. If no advice is available, click More Info to submit alert data to SmartDefense Advisor.

Select this check box before clicking Allow or Deny to avoid seeing an alert for this program again.

Figure 4-2: New Program alert

Some basics on responding to program alerts:

- By clicking **Allow**, you grant permission to the program.
- By clicking **Deny**, you deny permission to the program.
- If SmartDefense Advisor is set to "Auto," ZoneAlarm security software issues Program alerts only if no automatic setting is available.
- If you choose **Remember this setting** in a Program alert when allowing or denying program access, ZoneAlarm security software keeps your setting unless

SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

- If you do not choose **Remember this setting**, ZoneAlarm security software will issue another Program alert the next time the program attempts the same action.

See the topics below for more explanation and helpful tips about responding to and reducing each kind of program alert.

How do you know which type of program alert you are seeing on your system? Look at the name at the top of the program alert message.

- "New Program alert," on page 68
- "Repeat Program alert," on page 69
- "Changed Program alert," on page 69
- "Program Component alert," on page 70
- "Server Program alert," on page 71
- "Advanced Program alert," on page 73
- "Automatic VPN Configuration alert," on page 74
- "Manual Action Required alert," on page 74

New Program alert

New Program alerts enable you to set access permission for program that has not asked for Internet Zone or Trusted Zone access before. If you click Allow, the program is allowed access. If you click Deny, the program is denied access.

Why these alerts occur

New Program alerts occur when a program on your computer tries to initiate a connection with a computer in the Internet Zone or Trusted Zone, and that program has not already received access permission from you or, if you have enabled it, from SmartDefense Advisor.

As you begin to work with ZoneAlarm security software, you will probably see one or more New Program Alerts.

What you should do

Click Allow or Deny in the alert pop-up after answering these questions:

- Did you just launch a program or process that would reasonably require permission? If so, it's probably safe to click **Allow**. If not, continue.
- Do you recognize the name of the program in the Alert pop-up? If so, does it make sense for the program to need permission? If so, it's probably safe to click **Allow**. If not, or if you're not sure, continue.
- Click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the address it was trying to reach) to SmartDefense Advisor, which then displays a Web page with information about the alert and the program. Use the SmartDefense Advisor information to help you decide if it's safe to answer Allow.

If your browser does not have permission to access the Internet, you will be re-routed to this help file. To access SmartDefense Advisor, give your browser permission to access the Internet.

- If you're really not sure what to do, it's best to click **Deny**. You can always grant permission later by going to the Programs panel. "Setting permissions for specific programs," on page 101.

How to see fewer of these alerts

It's normal to see several New Program alerts soon after installing ZoneAlarm security software. As you assign permissions to each new program, the number of alerts you see will decrease. To keep from seeing Repeat Program alerts, select **Remember this setting** before clicking Allow or Deny.

If SmartDefense Advisor is set to "Auto," ZoneAlarm security software issues Program alerts only if no automatic setting is available. If you choose **Remember this setting** in a Program alert when allowing or denying program access, ZoneAlarm security software keeps your setting unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

Repeat Program alert

Repeat Program alerts occur when a program on your computer tries to initiate a connection with a computer in the Internet Zone or Trusted Zone, and that program has asked for permission before.

Why these alerts occur

If you respond Allow or Deny to a New Program alert without checking **Remember this answer**, you'll see a Repeat Program alert the next time the program asks for access permission.

What you should do

You should respond to Repeat Program alerts in the same way you would to New Program alerts. See "New Program alert," on page 68.

How to see fewer of these alerts

To keep from seeing Repeat Program alerts, select **Remember this setting** before clicking Allow or Deny in any New Program or Repeat Program alert. This sets the permission for the program to Allow or Block in the Programs panel.

If SmartDefense Advisor is set to "Auto," ZoneAlarm security software issues Program alerts only if no automatic setting is available. If you choose **Remember this setting** in a Program alert when allowing or denying program access, ZoneAlarm security software keeps your setting unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

Changed Program alert

Changed Program alerts warn you that a program that has asked for access permission or server permission before has changed somehow. If you click Allow, the changed program is allowed access. If you click Deny, the program is denied access.

Why these alerts occur

Changed Program alerts can occur if you have updated a program since the last time it accessed the Internet. However, they can also occur if a hacker has somehow managed to tamper with the program.

Remember, some programs are configured to access the Internet regularly to look for available updates. Consult the documentation for your programs, or refer to the support Web sites of their vendors, to find out if they have automatic update functionality.

What you should do

To determine how to respond to a Changed Program alert, consider these questions:

- Did you (or, if you're in a business environment, your systems administrator) recently upgrade the program that is asking for permission?

- Does it make sense for the program to need permission?

If you can answer "yes" to both questions, it's probably safe to click **Allow**.

If you're not sure, it's safest to click **Deny**. You can always grant permission later by going to the Programs panel. See "Setting permissions for specific programs," on page 101.

How to see fewer of these alerts

Changed Program alerts are always displayed because they require a Allow or Deny response from you. If you are using a program whose checksum changes frequently, you can avoid seeing numerous alerts by having ZoneAlarm security software check the program's file name only. "Adding a program to the programs list," on page 105.

Program Component alert

Use the Program Component alert to allow or deny Internet access to a program that is using one or more components that haven't yet been secured by ZoneAlarm security software. This helps protect you from hackers who try to use altered or faked components to get around your program control restrictions.

By clicking Allow, you allow the program to access the Internet while using the new or changed components. By clicking Deny, you prevent the program from accessing the Internet while using those components.

Why these alerts occur

Program Component alerts occur when a program accessing the Internet or local network is using one or more components that ZoneAlarm security software has not yet secured, or that has changed since it was secured.

ZoneAlarm security software automatically secures the components that a program is using at the time you grant it access permission. This prevents you from seeing a Component alert for every component loaded by your browser. To learn how ZoneAlarm security software secures program components, see "Managing program components," on page 110.

What you should do

The proper response to a Program Component alert depends on your situation. Consider the following questions:

- Are any of the following true?
  - You just installed or reinstalled ZoneAlarm security software.
  - You recently updated the application that is loading the component (For the application name, look under Technical Information in the alert pop-up.)
  - The application that is loading the component has an automatic update function.

- Someone else (for example, a systems administrator at your workplace) may have updated a program on your computer without your knowledge.

- Are you actively using the application that loaded the component?

If you can answer "yes" to both questions, it is likely that ZoneAlarm security software has detected legitimate components that your browser or other programs need to use. It is probably safe to answer Allow to the Program Component alert.

By clicking Allow, you allow the program to access the Internet while using the new or changed components. If you cannot answer yes both questions, or if you feel unsure about the component for any reason, it is safest to click Deny.

By clicking Deny, you prevent the program from accessing the Internet while using those components.

If you're not sure what to do, or if you decide to click **Deny**, investigate the component to determine if it is safe.

How to see fewer of these alerts

You may receive a large number of component alerts if you raised the Program Authentication level to high soon after installing ZoneAlarm security software. With authentication set to High, ZoneAlarm security software cannot automatically secure the large number of DLLs and other components commonly used by browsers and other programs.

To reduce the number of alerts, lower the authentication level to medium for the first few days after installing ZoneAlarm security software.

If you have been using ZoneAlarm security software for more than a few days, it is very rare to see large numbers of program alerts.

Server Program alert

Server Program alerts enable you to set server permission for a program on your computer.

Why these alerts occur

Server Program alerts occur when a program on your computer wants server permission for either the Internet Zone or Trusted Zone, and that program has not already received server permission from you. A program is acting as a server when it is open to receive connection requests from other computers. Several common types of applications, such as chat and e-mail programs may need to act as servers to operate

properly. However, some hacker programs act as servers to receive for instructions from their creators.

Relatively few programs on your computer will require server permission. Some common types of programs that do are:

- Chat
- Internet Call Waiting
- Music file sharing
- Streaming Media (such as RealPlayer)
- Voice-over-Internet
- Web meeting

If you are using the types of programs described above that require server permission to operate properly, grant permission before you start using the program. See "Granting a program permission to act as a server," on page 106.

If your browser does not have permission to access the Internet, you will be re-routed to the online help. To access SmartDefense Advisor, give your browser permission to access the Internet. See "Granting a program permission to access the Internet," on page 106.

What you should do

Before responding to the Server Program alert, consider the following:

- Did you just launch a program or process that would reasonably require permission? If so, it's probably safe to click Allow. If not, continue.
- Do you recognize the name of the program in the alert pop-up, and if so, does it make sense for the program to need permission? If so, it's probably safe to click Allow.
- Click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the address it was trying to reach) to SmartDefense Advisor, which then displays a Web page with information about the alert and the program. Use the SmartDefense Advisor information to help you decide if it's safe to answer Allow. For more information, see "Using SmartDefense Advisor and Hacker ID," on page 191.
- If you are still not certain that the program is legitimate and needs server permission, it is safest to click Deny. If it becomes necessary, you can give the program server permission later by using the Programs panel. See "Granting a program permission to act as a server," on page 106.

How to see fewer of these alerts

If you are using the types of programs described above that require server permission to operate properly, use the Programs panel in ZoneAlarm security software to grant permission before you start using the program. If you're seeing many server program alerts, you may want to run an virus scan as an added precaution.

Advanced Program alert

Advanced Program alerts are similar to other Program alerts (New Program, Repeat Program, and Changed Program)—they inform you that a program is attempting to access the network.

However, they differ from other Program alerts in that the program is attempting to use another program to connect to the Internet, or is attempting to manipulate another program's functionality.

Why these alerts occur

Advanced Program alerts occur in two situations: when a program on your computer tries to initiate a connection with a computer in the Internet Zone or Trusted Zone by instructing another program to connect; or when a program attempts to hijack the processes of another program by calling the OpenProcess function.

There are some legitimate programs associated with your operating system that may require access to another program. For example, if you were using Windows Task Manager to shutdown Internet Explorer, Windows Task Manager would need to call the OpenProcess function on the Internet Explorer program in order to shut it down.

What you should do

How you should respond to an Advanced Program alert depends upon the cause of the alert. If the Advanced Program alert was caused by the OpenProcess function being called, you should determine whether the function was called by a legitimate program or by a malicious one. Verify that the program cited in the alert is one you trust to carry out this function. For example, if you were attempting to shut down a program using Windows Task Manager when you received the Advanced Program alert, it is probably safe to answer **Allow**. Similarly, if the alert was caused by a program using another program to access the Internet and that program routinely requests such permission, is probably safe to answer **Allow**. If you are unsure as to the cause of the alert or the expected behavior of the program initiating the request, it is safest to click **Deny**. After denying advanced permission to the program, perform an Internet search on the program's file name. If the program is malicious, it is likely that information about it is available, including how to remove it from your computer.

How to see fewer of these alerts

It is unusual to see a large number of Advanced Program alerts. If you receive repeated alerts, research the program name or names and consider either removing the program from your computer or providing the program with the necessary access rights.

Automatic VPN Configuration alert

Automatic VPN Configuration alerts occur when ZoneAlarm security software detects VPN activity. Depending upon the type of VPN activity detected, and whether ZoneAlarm security software was able to configure your VPN connection automatically, you may see one of three Automatic VPN Configuration alerts.

Why these alerts occur

Automatic VPN Configuration alerts occur when ZoneAlarm security software detects VPN activity that it is not configured to allow.

What you should do

How you should respond to an Automatic VPN Configuration alert depends upon which Automatic VPN Configuration alert you encounter, whether you are running VPN software or not, and whether you want to configure ZoneAlarm security software to allow your VPN connection.

If you have created an expert firewall rule that blocks VPN traffic, you will need to modify the expert rule to allow VPN traffic. See "Creating expert firewall rules," on page 48.

- If you are running VPN software on your computer and you want to configure the connection, select either:

  Configure ZoneAlarm security software to support this VPN connection, or

  I am running VPN software and would like to configure ZoneAlarm security software to support it

- If are running VPN software but do not want ZoneAlarm security software to configure your connection, select **Do not configure ZoneAlarm security software to support this VPN connection**.

- If you are not running VPN software, select **I am not running VPN software**.

How to see fewer of these alerts

If you are running VPN software, the only way to see fewer of these alerts is to properly configure your ZoneAlarm security software to allow your VPN software and its required resources. See "Configuring your VPN connection manually," on page 29.

Manual Action Required alert

A Manual Action Required alert informs you that further steps must be taken before ZoneAlarm security software is properly configured to support your VPN connection.

Why these alerts occur

A Manual Action Required alert occurs when ZoneAlarm security software is unable to configure your VPN connection automatically, or if further manual changes are required before automatic configuration can be completed.

What you should do

Manual Action Required alerts do not require a response from you. To configure VPN connection manually, see "Configuring your VPN connection manually," on page 29 and follow the instructions for manual configuration.

How to see fewer of these alerts

It is unusual for you to see many Manual Action Required alerts. If you do see multiple alerts, either perform the required steps to properly configure your ZoneAlarm security software to support your VPN connection, or remove the VPN software from your computer.

OSFirewall alerts

OSFirewall alerts are alerts that appear when programs or processes on your computer are attempting to modify your computer's settings or programs.

There are three types of OSFirewall alerts, two of which require a response from you: Medium-rated Suspicious and High-rated Suspicious. Malicious alerts do not require a response from you.

- Medium-rated Suspicious Behavior alert
- High-rated Suspicious Behavior alert
- Malicious behavior alert

Medium-rated Suspicious Behavior alert

Medium-rated Suspicious Behavior alerts inform you that a trusted program is trying to perform an action that may change the default behavior of a program. For example, if a program were to modify your browser's home page, you would see a Medium-rated Suspicious Behavior alert. If you click Allow, the program is allowed to perform the activity. If you click Deny, the program is prevented from performing the activity and is

given Restricted access, which means that all future suspicious behavior will be denied.

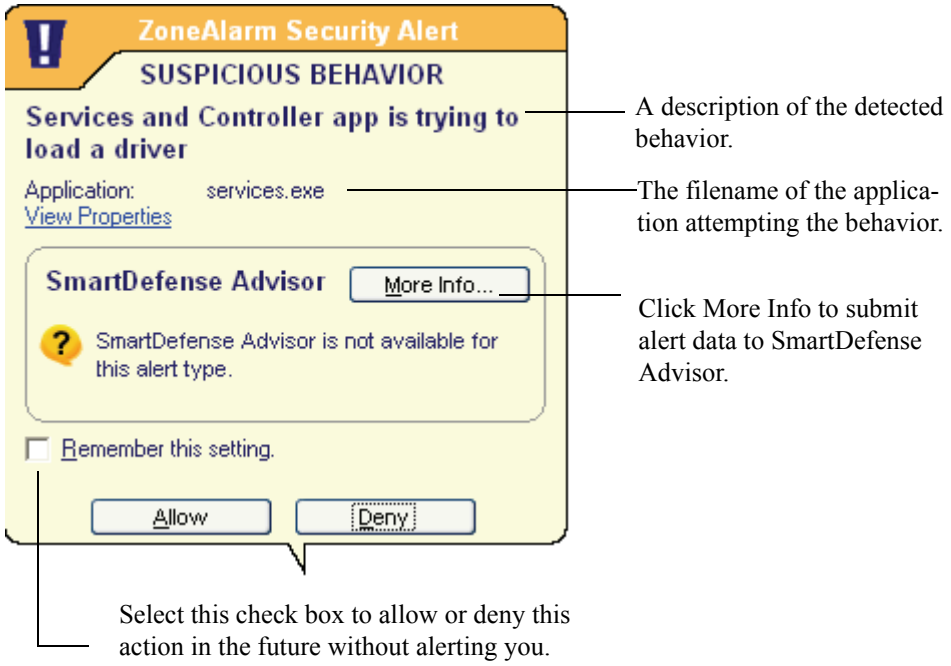


Figure 4-3: Medium-rated Suspicious Behavior alert

Why these alerts occur

Hackers often use trusted programs to modify other programs, such as your browser settings or to compromise your computer's operating system.

What you should do

Click **Allow** or **Deny** to respond. If you are not sure whether to allow or deny the action, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

The table below also provides some information you can use to determine how to respond to Medium-rated Suspicious Behavior alerts when they appear. The information listed here is for your reference only. Bear in mind that some legitimate programs need to perform the actions listed below. Whether to allow or deny suspicious program behavior should be determined by your individual situation. (Note that you can

configure ZoneAlarm security software to prevent several of these behaviors automatically. For details, see "Configuring OSFirewall protection," on page 96.) .

Detected Behavior	What this means	Considerations
Modifications of the startup directory	A program is setting itself to run each time your computer is started.	Unless you are installing a program, you should deny this action, as it could be spyware.
Modification of browser search defaults	Your default browser search is being modified.	Unless you are currently modifying your browser's search function, you should deny this action.
Modification of browser page defaults	Your default browser home page is being modified.	Unless you are changing your home page, you should deny this action.
Unloading of driver	A program is trying to trying to unload another program's driver.	There are no legitimate reasons for this behavior. You should deny this action.

Table 4-4: Medium-rated suspicious behavior guide

Selecting **Remember this setting** before clicking Allow or Deny causes ZoneAlarm security software to remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, and you select **Remember this setting** in an OSFirewall alert, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

High-rated Suspicious Behavior alert

A High-rated Suspicious Behavior alert informs you that a program on your computer is attempting activity that could be dangerous.

Examples of such behaviors include:

- attempts to access a disk without going through the file system. This behavior is used by malicious software to get around file protection by changing raw data on your disk.
- behavior that may cause programs or your operating system to stop functioning normally
- behaviors that indicates spyware is trying to monitor your activity

If you click Allow, the program is allowed to perform the activity. If you click Deny, the program is prevented from performing the activity and is given Restricted, access which means that all future suspicious behavior will be denied.

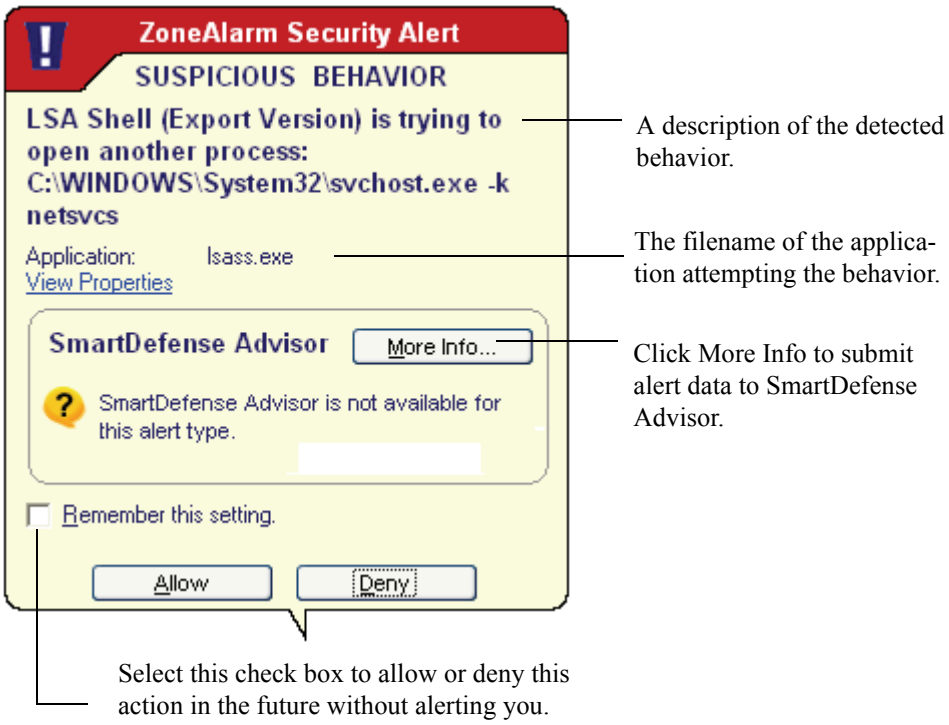


Figure 4-5: High-rated Suspicious Behavior alert

Why these alerts occur

These alerts occur when a program or component on your computer was detected trying to hijack a process or program on your computer, to alter default settings on your computer or one of its programs, or access a file without going through the standard protected file system.

What you should do

Because of the nature of the actions that cause a High-rated Suspicious Behavior alert to appear, it's safest to click Deny in the alert pop-up. If you're not sure, click the **More Info** button in the alert box. This submits your alert information (for example, the name of the program and the activity it was trying to perform) to SmartDefense Advisor, which then displays a Web page with information about the alert and the behavior. Use the SmartDefense Advisor information to help you decide whether to allow or deny the action.

Be aware, however, that some legitimate programs perform behavior of this kind as part of normal program functioning. If you trust the program requesting permission, then it may be safe to allow this behavior. In such cases, denying the behavior may result in interrupted program activity.

The table below provides some information you can use to determine how to respond to High-rated Suspicious Behavior alerts when they appear. The information listed here

is for your reference only. Bear in mind that few legitimate programs need to perform the actions listed below.

Selecting **Remember this setting** before clicking Allow or Deny causes ZoneAlarm security software to remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, and you select **Remember this setting** in an OSFirewall alert, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

Detected Behavior	What this means	Recommendation
Transmission of DDE (Dynamic Data Exchange) input	Program is trying to send DDE input to another program, which could allow the program to gain Internet access or to leak information.	This behavior is often used to open URLs in Internet Explorer. If the application performing the behavior is known and trusted, it is probably safe to allow the behavior. Otherwise, click Deny.
Sending Windows messages	A program is trying to send a message to another program.	A program could be trying to force the another program to perform certain functions. Unless you are installing software that needs to communicate with another program, you should deny this action.
A program is trying to kill another program.	A program is trying to terminate another program	A program could be trying to kill a trusted program. Unless you have just used Task Manager to end a program or process, or have just installed software that requires a reboot of your computer, you should deny this action.
Invoking open process/thread	A program is trying to control another program. It is legitimate for system applications to do this.	Unless the program performing the behavior is trusted, you should deny this action.
Monitoring keyboard and mouse input	A program is attempting to monitor your keyboard strokes and mouse input.	Unless you are running a specialized program that needs to monitor this activity in order to function, such as narration software, you should deny this action.

Table 4-6: High-rated suspicious behavior guide

Detected Behavior	What this means	Recommendation
Remote control of keyboard and mouse input	A program is attempting to remotely control your keyboard and mouse.	Unless you are running remote-access software, such as PC Anywhere or VNC, you should deny this action.
Installation of driver	A program is attempting to load a *driver*. Loading a driver allows a program to do anything it wants on your computer.	Unless you are installing anti-virus, anti-spyware, firewall, VPN, or other system tools, you should deny this action.
Modification of *physical memory*	A program may be attempting to modify or read information owned by another program.	Unless you are running gaming, video, or system utility software, you should deny this action.
Injection of code into a program or system service	A program is attempting to inject code into another program, which can be used to disable the program or service.	Unless you are running highly specialized software to change the appearance or behavior of a program, you should deny this action.
Modifying network parameters	A program is attempting to change your network settings, possibly to re-route you to dangerous Web sites and monitor your Web traffic.	Unless you are running TCP/IP tuning software, you should deny this action.
Launching an unknown or bad program from a good one	A program is attempting to modify another program.	Unless a program you are using has a reason to open another program (such as a Word document with a link to a browser, or an IM program with links to other programs) you should deny this action.
Accessing system registry	The process is trying to modify registry settings.	This behavior is usually blocked automatically. If you have program control set to Manual mode, deny this action.
Deletion of a run key	A program was trying to delete a run key entry.	If the program was set to launch on start-up but was cancelled, it will delete the run key. In other cases, you should deny this action.

Table 4-6: High-rated suspicious behavior guide

Detected Behavior	What this means	Recommendation
Modification of ZoneAlarm program	A program is trying to modify the ZoneAlarm program, possibly to prevent it from running, or performing product updates.	Unless you are upgrading the ZoneAlarm client, deny this action.

Table 4-6: High-rated suspicious behavior guide

Selecting **Remember this setting** before clicking Allow or Deny causes ZoneAlarm security software to remember your setting and apply it automatically when the program attempts another similar action. If SmartDefense Advisor is set to Auto, and you select **Remember this setting** in an OSFirewall alert, your setting will remain effective unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

.

Malicious behavior alert

A Malicious Behavior alert informs you that a malicious program is attempting to run on your computer. Programs that are designated by ZoneAlarm security experts tend to be known worms, viruses, trojans, or other such malware.

Why these alerts occur

These alerts inform you that a program on your computer will be killed (shut down).

What you should do

Malicious alerts do not require a response from you. They merely inform you of an action that is taking place. If a trustworthy program is mistakenly killed, you can enable the program from the Programs List.

ID Lock alert

An ID Lock alert informs you that information stored in myVAULT is about to be sent to a destination that is not on the Trusted Sites list.

If they have enabled the ID Lock feature, users may see ID Lock alerts if the personal information stored in myVAULT is sent to a destination that is not listed on their Trusted Sites list.

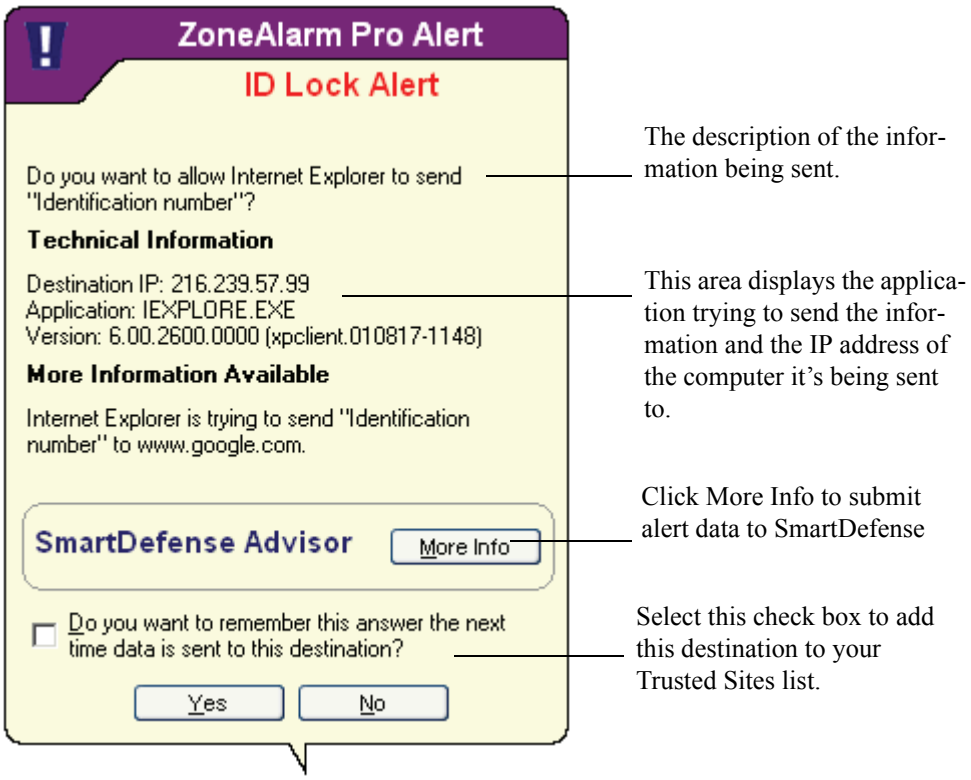


Figure 4-7: ID Lock alert

Why these alerts occur

An ID lock alert occurs when information stored in myVAULT is either entered into a Web page or e-mail message, or when your password is being sent to a destination in clear text (unencrypted) form without your authorization.

What you should do

By clicking the Yes button, you grant permission to send the information to the requesting IP address. If you do not want to be alerted the next time myVAULT data is sent to this destination, select the **"Do you want to remember..."** check box to add the destination to your Trusted Sites list.

You should determine whether the site requesting the information is one that you trust. Whether you should allow or block the information depends upon the sensitivity of the

information, the legitimacy of the request, and the authenticity of the site. If you are in the process of making an online purchase with a trustworthy vendor when you see the alert, it's probably safe to let the information go through. If you see an alert requesting your information when you are not performing such a transaction, it's safest to block the transmission.

Additionally, a few sites transmit passwords in clear text format. If you were to block clear text passwords for a site, then visit that site and enter your password, you would see an ID Lock alert.

How to see fewer of these alerts

You may see frequent ID lock alerts if you frequently submit myVAULT contents to sites that you have not entered on the Trusted Sites list, or if you have blocked clear text passwords for a site that uses clear text passwords. You can minimize the number of ID Lock alerts by adding sites to the Trusted Sites list with which you frequently share your personal information, and by allowing clear text passwords for those sites that use them.

New Network alerts

A New Network alert appears when ZoneAlarm security software detects that you're connected to a network you haven't seen before—be it a wireless home network, a

business LAN, or your ISP's network. You can use the alert pop-up to enable file and printer sharing with that network.

The first time you use ZoneAlarm security software, you will almost certainly see a New Network alert. Don't worry! This alert is a convenience tool designed to help you configure ZoneAlarm security software.

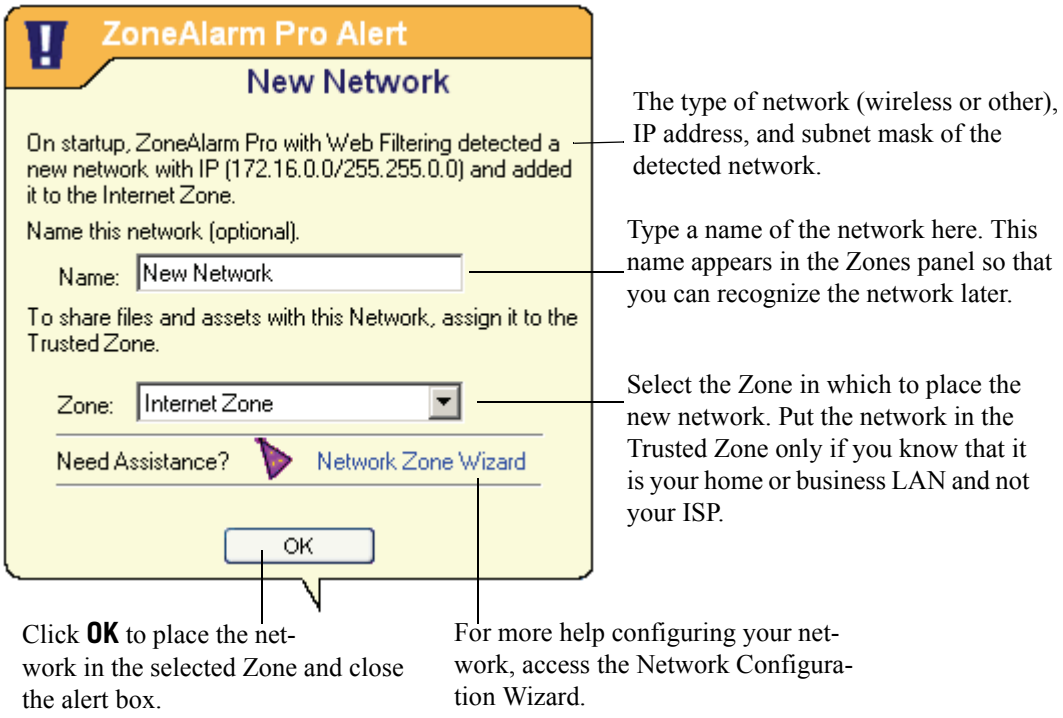


Figure 4-8: New Network alert

Why these alerts occur

New Network alerts occur when you connect to any network—be it a wireless home network, a business LAN, or your ISP's network.

What you should do

How you respond to a New Network alert depends on your particular network situation.

If you are connected to a home or business local network and you want to share resources with the other computers on the network, put the network in the Trusted Zone.

To add the new network to the Trusted Zone:

1. In the New Network alert pop-up, type a name for the network (for example "Home NW") in the Name box.
2. Select **Trusted Zone** from the Zone drop-down list.

3. Click **OK**.

If you are not certain what network ZoneAlarm security software has detected, write down the IP address displayed in the alert box. Then consult your home network documentation, systems administrator, or ISP to determine what network it is.

Use caution if ZoneAlarm security software detects a wireless network. It is possible for your wireless network adapter to pick up a network other than your own. Be sure that the IP address displayed in the New Network alert is your network's IP address before you add it to the Trusted Zone.

If you are connected to the Internet through a standard modem and dial-up connection, a Digital Subscriber Line (DSL), or a cable modem, click **OK** in the New Network alert pop-up.

If you click Cancel, ZoneAlarm security software will block your Internet connection. Do not add your ISP network to the Trusted Zone.

How to see fewer of these alerts

It is unusual to receive a lot of New Network alerts.

Chapter 5

Program Control

Program control and SmartDefense Advisor work together to keep bad programs on your PC from accessing the Internet while making sure that good programs have the access they need. You can assign program control permissions manually or let ZoneAlarm security software assign permissions when program advice is available. Advanced users can control the ports that each program is permitted to use.

Topics:

- "Understanding Program Control," on page 89
- "Setting general program control options," on page 93
- "Setting permissions for specific programs," on page 101
- "Managing program components," on page 110
- "Creating expert rules for programs," on page 111

Understanding Program Control

Your outbound protection is called program control. Everything you do on the Internet—from browsing Web pages to downloading audio files—is managed by specific programs on your computer. Hackers exploit this fact by planting "malware"—malicious software—on your computer. Malware can masquerade as harmless e-mail attachments or as updates to

legitimate programs. Once on your computer, however, the malware can hijack trusted programs and carry out malicious activities under the guise of legitimacy.

ZoneAlarm security software protects your computer from hackers and malicious attacks by assigning policies to programs that indicate their level of trustworthiness and specify the actions they are allowed to perform.

Some versions of ZoneAlarm security software include OSFirewall protection, which detects when programs try to use your operating system to perform suspicious actions on your computer.

The minimum you need to know about program control

- By default, a program's permission to access the Internet is automatically determined by SmartDefense Advisor.
- Alerts appear if SmartDefense Advisor is unfamiliar with a program. (When the unknown program wants access the Internet for the first time, a **New Program alert** asks if you want to grant the access.)
- If a program is trying to *act as a server,* a **Server Program alert** asks you if you want to grant server permission. A program "acts as a server" when it is open to receive connection requests from other computers. Though some applications, such as e-mail programs, may need to act as servers to operate, hacker programs act as servers to receive instructions from their creators. Be careful to give server permission only to programs that you trust and that need server permission to operate.
- To avoid seeing numerous alerts for the same program, select the **Remember this answer** check box before clicking Yes or No in an alert. After that, the program will be automatically blocked or allowed.
- You can control the Internet and server permissions for specific programs by using the Program Control panel or by allowing program control to ask you about each program as it is activated.

Next topics:

Setting program permissions automatically

Setting program permissions manually

Setting program permissions automatically

The SmartDefense Advisor and Program Control settings work together to ensure that good programs are given network access and that bad programs are denied access. By default, Program Control is set to Medium and SmartDefense Advisor is set to Auto. With these defaults, ZoneAlarm security software assigns permission to programs

automatically. For information about customizing Program Control and SmartDefense Advisor, see "Setting general program control options," on page 93.

If SmartDefense Advisor and Program Control are set to their defaults, one of three things may occur when a program requests access for the first time:

- Access is granted - Access is granted if the program is known to be safe and requires the permissions it is asking for in order to function properly.
- Access is denied - Access is denied if the program is a known bad program or if the program does not require the permissions it is asking for.
- A New Program alert appears - Program alerts appear when you need to decide whether to allow or deny Internet access to a program. The alert may contain a recommendation about whether to allow or deny access, and, if necessary, you can click **More info** to get details about the program to help you respond.

  As long as SmartDefense Advisor is set to Auto, you see a program alert only if there is no automatic setting available. If you choose **Remember this setting** in a Program alert when allowing or denying program access, ZoneAlarm security software keeps your setting unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel. For more information about different types of Program alerts, see "Program alerts," on page 65

Safe programs

ZoneAlarm security software validates your programs against a database of known safe programs and automatically assigns the permissions required for the programs to function properly. If you accepted the default program settings in the Configuration Wizard, ZoneAlarm security software is set up to automatically configure the most popular programs in the following general categories:

- Browsers (e.g., Internet Explorer, Netscape)
- E-mail applications (e.g., Microsoft Outlook, Eudora)
- Instant Messengers (e.g., AOL, Yahoo!)
- Anti-virus (e.g., Symantec, ZoneAlarm)
- Document utilities (e.g., WinZip® and Adobe® Acrobat®)
- ZoneAlarm software applications

Even programs that are considered safe can be used by hackers to perform actions that are not. OSFirewall protection displays alerts when it detects suspicious program behavior. For more information about these alerts, see "Program alerts," on page 65.

Setting program permissions manually

If you want to assign permissions to programs on your own, or if ZoneAlarm security software was unable to assign permissions automatically, you can set permissions

manually by using Program alerts, or by setting permissions for specific programs on the Program Control | Programs panel.

Program alerts

When a program requests access for the first time, a New Program alert asks you if you want to grant the program access permission. When a program is detected to be listening to the ports on your computer, a Server Program alert is displayed.

Suspicious behavior alerts inform you that a trusted or unknown program on your computer is trying to perform an action that could be considered suspicious.

To avoid seeing numerous alerts for the same program, select **Remember this setting** before clicking **Allow** or **Deny**. ZoneAlarm security software will continue to apply your Allow or Deny setting (without issuing alerts) unless you set SmartDefense Advisor to Auto and it has a setting different from yours.

Because Trojan horses and other types of malware often need server rights in order to do mischief, you should be particularly careful to give server permission only to programs that you know and trust, and that need server permission to operate properly. Several common types of applications, such as chat programs, e-mail clients, and Internet Call Waiting programs, may need server permission to operate properly. Grant server permission only to programs you're sure you trust, and that require it in order to work.

If possible, avoid granting a program server permission for computers in your firewall Internet Zone. If you need to accept incoming connections from only a small number of machines, add those machines to your firewall Trusted Zone, and then allow the program server permission for the Trusted Zone only.

For more information about program alerts, see "Program alerts," on page 65.

You also can allow ZoneAlarm security software to automatically allow or deny all new programs without displaying an alert. For example, if you are sure you have given access permission to all the programs you want, you might automatically deny access to any other program that asks for permission. For more information, see "Setting permissions for specific programs," on page 101.

Programs list

The Programs list allows you to set or customize permissions for specific programs based on your individual needs. For more information about using the Programs list and customizing permissions, see "Using the programs list," on page 102.

Setting general program control options

When you're using ZoneAlarm security software, no program on your computer can access the Internet or your local network, or act as a server, unless it has permission to do so.

- Setting the program control level
- Custom program control features
- Configuring OSFirewall protection
- Enabling Component Control
- Understanding services control
- Setting the SmartDefense Advisor level
- Enabling the automatic lock
- Viewing logged program events

Setting the program control level

ZoneAlarm security software offers several methods of program control:

- Basic program control lets you determine access and server rights for individual programs.
- The Custom Program Control Settings window provides several high-security settings that are designed to prevent malicious programs from controlling trusted programs. See "Custom program control features," on page 95.
- OSFirewall protection detects when programs try to use your operating system to perform suspicious actions on your computer. For details on OSFirewall, see "Configuring OSFirewall protection," on page 96.

Understanding Auto-Learn

Auto is the default setting for the first 21 days of using ZoneAlarm security software. ZoneAlarm security software observes and tracks which safe programs you use regularly, so that you are not interrupted with alerts about these programs. After this self-learning period, a message appears asking you whether you would like to continue in Auto learning mode or move program control level to Max so that you have maximum outbound protection.

To set the program control level:

1. Select **Program Control**.

2. In the Program Control area, click the slider and drag it to the desired setting.

Max (for versions with Anti-virus) High (for versions without Anti-virus)	With this setting, you may see a large number of alerts. ◆ Programs must ask for Internet access and server rights. ◆ OSFirewall will monitor for suspicious behaviors, including attempts to get around file system controls by accessing raw disk data. ◆ Advanced Program control and Application Interaction Control are enabled. ◆ Service control manager is on if you have enabled it in the Custom program control settings. ◆ By default, component control is disabled.*
Auto (for versions with Anti-virus)	This Auto-Learn mode minimizes alerts by recognizing your frequently used programs and giving them network access without interrupting your work with frequent alerts ◆ This is the default level for the first 21 days. Most program alerts are suppressed by giving access to programs you frequently use and relying on SmartDefense Advisor to screen programs ◆ The OSFirewall will also screen some programs. ◆ Not as secure as the Max or High setting.
Medium (for versions without Anti-virus)	This is the default setting. ◆ Programs must ask for Internet access and server rights. ◆ OSFirewall will monitor for suspicious behaviors. ◆ By default, component control is disabled.*
Min (for versions with Anti-virus)	◆ OSFirewall is disabled. ◆ By default, component control is disabled.* ◆ Server control and stealth mode are available
Low (for versions without Anti-virus)	◆ OSFirewall is disabled. ◆ By default, component control is disabled.* ◆ Server control and stealth mode are not available
Off	Program control is disabled. ◆ No programs or components are authenticated or learned. ◆ No program permissions are enforced. ◆ All programs are allowed access/server rights. ◆ All programs are allowed to perform suspicious behavior. ◆ No program alerts are displayed.

* Component control is disabled by default. If you have turned component control on, it will remain enabled as long as program control is set to High, Medium, or Low. For informa-

tion about component control, including directions for turning it on, see "Enabling Component Control," on page 97.

To limit the number of alerts you see, you can use the following features:

- Use the **Auto** program control level, which employs the *Auto-Learn* feature.
- Leave SmartDefense Advisor on the Auto setting, to benefit from automatic program settings.

Custom program control features

The Custom Program Control Settings window provides several high-security settings that are designed to prevent malicious programs from controlling trusted programs.

1. Select **Program Control**, and then click the **Custom** button.
2. Specify the settings to apply.

Enable Advanced Program Control	Prevents trusted programs from being used by untrusted programs to circumvent outbound firewall protection.
Enable Application Interaction Control	Alerts you when a process attempts to use another process or when a program launches another program.
Enable Timing Attack Prevention	Detects and stops programs that try to hijack a trusted program's permissions (e.g., to load drivers, change registry keys, or regulate processes). Also known as handle protection. On by default when Program Control is High or Maximum.
Enable Microsoft Catalog Utilization	When enabled, prevents alerts for programs that are cataloged by Windows as known and trustworthy. Enabled by default. (Depending on your settings, ZoneAlarm may still alert you about such programs if they attempt to act as a server outside your Trusted Zone.)
Enable component control	Restricts or monitors individual components, such as DLL files or ActiveX controls, that malware programs may use to access the network. If program control is Medium, component control tracks components but does not restrict them. If program control is High, it prompts you to allow or deny new components. See "Enabling Component Control," on page 97 for details.

Enable services control	Alerts you if untrusted programs attempt to install or modify a service or driver. Active when Program Control is set to High or Maximum. See"Understanding services control," on page 96 for more information.

3. Click **OK**.

To learn about the settings on the OSFirewall panel of this dialog, see "Configuring OSFirewall protection," on page 96.

Since some programs that control other programs are legitimate, ZoneAlarm gives the most common ones permission to access the Internet. You can view and adjust individual configurations on the Programs panel.

Configuring OSFirewall protection

OSFirewall protection, which is enabled by default, detects when programs try to use your operating system to perform suspicious and potentially damaging actions on your computer. You can also configure various OSFirewall Special System Protections, which determine whether programs on your computer can perform specific actions such as modifying your Internet Explorer home page or installing ActiveX controls.

See "OSFirewall alerts," on page 75 for more details about the kinds of behaviors and alerts that are associated with OSFirewall protection.

To configure OSFirewall settings:

1. Select **Program Control**.
2. In the Program Control area, click **Custom**.
3. In the dialog that appears, select the **OSFirewall** panel.
4. Select or deselect **Enable OSFirewall**, as desired. (To configure any OSFirewall Special System Protections in the next step, you must first enable OSFirewall.)
5. Optionally, configure any OSFirewall Special System Protections. For any action in the list, click the State field and select **Allow**, **Deny**, **Ask**, or **Use Program Setting**. If you choose Use Program Setting, ZoneAlarm security software defers to SmartDefense Advisor settings or to your manual settings.
6. Click **Apply** to save the setting and leave the dialog open, or **OK** to save the setting and close the dialog.

Understanding services control

The services control feature catches dangerous program behaviors that other firewalls have typically ignored. It controls changes to the Windows Services section of your computer's registry file, blocking attempts by untrusted programs to install or modify

services or drivers. If such attempts occur, you are alerted and given the choice to allow or deny them.

This protection:

- prevents malware from being installed to start automatically when your computer starts up
- prevents drivers from being loaded into your PC kernel by rootkit malware

You can enable or disable services control in the Program Control Custom Settings window, as described in "Custom program control features," on page 95. Services controls activates only when Program Control is set to High or Maximum.

Another Windows component monitored by program control is Component Object Model (COM). Drive-by downloads from websites may try to use COM to gain access for taking data from your computer, but ZoneAlarm prevents this by monitoring COM for suspicious behavior. This protection is always enabled.

Enabling Component Control

In addition to controlling permissions for all *programs* on a computer, advanced users may also want to monitor and, if desired, restrict individual *components* that these programs load (such as DLL files or ActiveX controls). ZoneAlarm security software keeps a list of components (used by allowed programs) that have tried to access the Internet or the local network. Depending on your program control and component control settings, ZoneAlarm security software can simply monitor components or it can alert you each time a new component attempts access. This section explains how to enable component control. For details about viewing the Components List and modifying component permissions manually, see "Managing program components," on page 110.

By default, component control is turned off, though ZoneAlarm security software does add components to the Components List. If you enable component control and set program control to Medium, component control tracks components but does not restrict their activity. If you then reset program control to High, component control grants access to all previously known components but prompts you to allow or deny any components discovered subsequently. For advanced users concerned about component activity, the best practice is to install ZoneAlarm security software on a freshly set up computer, enable component control and set the program control level to Medium, and, after ZoneAlarm security software has had a chance to detect all normal components that require access, reset program control to High. (For information about the program control setting, see "Setting the program control level," on page 93.)

To enable component control:

1. Select **Program Control**.
2. In the Program Control area, click **Custom**.

   The Custom Program Control Settings dialog appears.

3. On the Program Control panel, select **Enable component control**.
4. Click **OK**.

Setting the SmartDefense Advisor level

Whenever you use a program that requests access, SmartDefense Advisor queries the ZoneAlarm server to determine the policy for that program. You can choose to have SmartDefense Advisor set the permissions for the program automatically, or you can configure program access manually. The SmartDefense Advisor level is set to Auto by default.

If you set SmartDefense Advisor to Auto and there is no advice available for a program, ZoneAlarm security software displays a Program alert prompting you to allow or deny access to the program. If you select **Remember this setting** when responding to such a Program alert, ZoneAlarm security software keeps your setting unless SmartDefense Advisor comes out with a different setting, or until you change the setting manually in the Programs panel.

For information about setting program permissions manually, see "Setting permissions for specific programs," on page 101. You can set SmartDefense Advisor to Manual or Off and set *all* program permissions manually. Or, you can set SmartDefense Advisor to Auto and set manual program permissions *only* when SmartDefense Advisor does not recommend a policy.

To set the SmartDefense Advisor level

1. Select **Program Control**.
2. In the SmartDefense Advisor area, choose your setting.

Auto	In Auto mode, SmartDefense Advisor automatically implements the recommendation returned from the server. Program Control must be set to Medium or High to set SmartDefense Advisor to Auto.
Manual	In Manual mode, you will receive Program alerts when programs request access and can set the permission on your own.
Off	SmartDefense Advisor will not contact the server for program advice.

Enabling the automatic lock

The automatic Internet lock protects your computer if you leave it connected to the Internet for long periods even when you're not actively using network or Internet resources.

When the lock engages, only traffic initiated by programs to which you have given pass-lock permission is allowed. All traffic to and from your computer is stopped, including DHCP messages, or ISP heartbeats, used to maintain your Internet connection. As a result, you may lose your Internet connection.

You can set the Internet lock to engage:

- When your screen saver engages, or
- After a specified number of minutes of network inactivity.

To enable or disable the automatic lock:

1. Select **Program Control**.
2. In the Automatic Lock area, select **On** or **Off**.

To set automatic lock options:

1. Select **Program Control**.
2. In the Automatic Lock area, click **Custom**.

   The Custom Lock Settings dialog appears.
3. Specify the lock mode to use.

Lock after n minutes of inactivity	Engages automatic lock after the specified number of minutes has passed. Specify a value between 1 and 99.
Lock when screensaver activates	Engages automatic lock whenever your screensaver is activated.

4. If desired, specify Internet access permissions for periods when the lock is engaged.

Allow pass-lock programs to access the Internet	Allows programs with pass-lock permission to access the Internet. Programs without pass-lock permission have no access. This is the default behavior when the lock is engaged.
Block all Internet access	Prevents all programs, regardless of pass-lock status, from accessing the Internet when the lock is engaged.

5. Click **OK**.

Viewing logged program events

By default, all Program events are recorded in the Log Viewer.

To view logged program events:

1. Select **Alerts & Logs | Log Viewer**.
2. Select **Program**, from the Alert Type drop-down list.

Table 5-1 provides an explanation of the log viewer fields available for Program events.

Field	Explanation
Rating	Event rating based on the **Protection Level** of the security option.
Date/Time	Date and time the event occurred.
Type	Type of program alert that occurred. Possible values for this column include: • Program Access • Repeat Program • New Program
Program	The program (displayed as the application file) that requested access. If a program name is unavailable, refer to the Description field of the Entry Details window.
Source IP	The IP address of the computer sending the request. If the source IP cannot be determined, this field may be left blank.
Destination IP	The IP address of the computer receiving the request. If the destination IP cannot be determined, this field may be left blank.
Direction	Specifies whether the request that caused the event was incoming, outgoing, or occurred as a result of internal traffic on your computer (data).
Action Taken	Specifies whether the request was Allowed or Blocked. Action is followed by /
Count	The number of times this action was taken.
Source DNS	The domain name server of the computer that is sending the request.
Destination DNS	The domain name server of the computer that is receiving the request.

Table 5-1: Program event log fields

Viewing logged OSFirewall events

By default, all OSFirewall events are recorded in the Log Viewer.

To view logged OSFirewall events:

1. Select **Alerts & Logs | Log Viewer**.
2. Select **OSFirewall**, from the Alert Type drop-down list.

Table 5-2 provides an explanation of the log viewer fields available for OSFirewall events.

Field	Explanation
Rating	Event rating based on the **Protection Level** of the security option.
Date/Time	Date and time the event occurred.
Type	Type of OSFirewall alert that occurred. Possible values for this column include: • Process • Message • Module • Registry • File • Execution • Driver • Physical memory
Subtype	The specific event that initiated the Type of access requested (for example, OpenThread would be a subtype of Process).
Data	The path to the file that was attempting to be modified.
Program	Displays the path to the program that performed the behavior.
Action Taken	Specifies whether the request was Allowed or Blocked. Action is followed by /manual or /auto to indicate whether the action was performed by you or by SmartDefense Advisor.
Count	The number of times this action was taken.

Table 5-2: OSFirewall event log fields

Setting permissions for specific programs

In some cases, you may want to specify different settings for an individual program than the global program control level will allow. For example, if you wanted to allow access to

a particular program, but keep security High for all other programs, you could set the permission for that program to **Allow**.

After you manually set permissions for a program, the permissions for that program will not change even if you later set the SmartDefense Advisor level to Auto. To benefit from automatic program advice, remove the program from the Programs List, then set the SmartDefense Advisor level to Auto.

- Using the programs list
- Adding a program to the programs list
- Granting a program permission to access the Internet
- Granting a program permission to act as a server
- Setting passlock permission for a program
- Granting send mail permission to a program
- Select Allow from the shortcut menu.

Using the programs list

The programs list provides an overview of the programs on your computer that have tried to access the Internet or the local network. For each program, the program list provides detailed information about its current state, trustworthiness, and the functions it is allowed to perform. The programs list is organized in alphabetical order. You can sort the programs in the list by any column by clicking on column header. As you use your computer, ZoneAlarm security software detects every program that requests network access and adds it to the programs list. To access the Programs List, select **Program Control | Programs**.

Selecting a program name in the list displays program information in the yellow Entry Detail area below the list. This area provides details about the program, including its full name, the program's OSFirewall policy, and the date of the last policy update.

The SmartDefense Advisor and Trust Level columns indicate OSFirewall Protection for your computer and specify whether a program is allowed to perform operating system-

level actions like changing TCP/IP parameters, loading or installing drivers, or changing your browser's default settings.

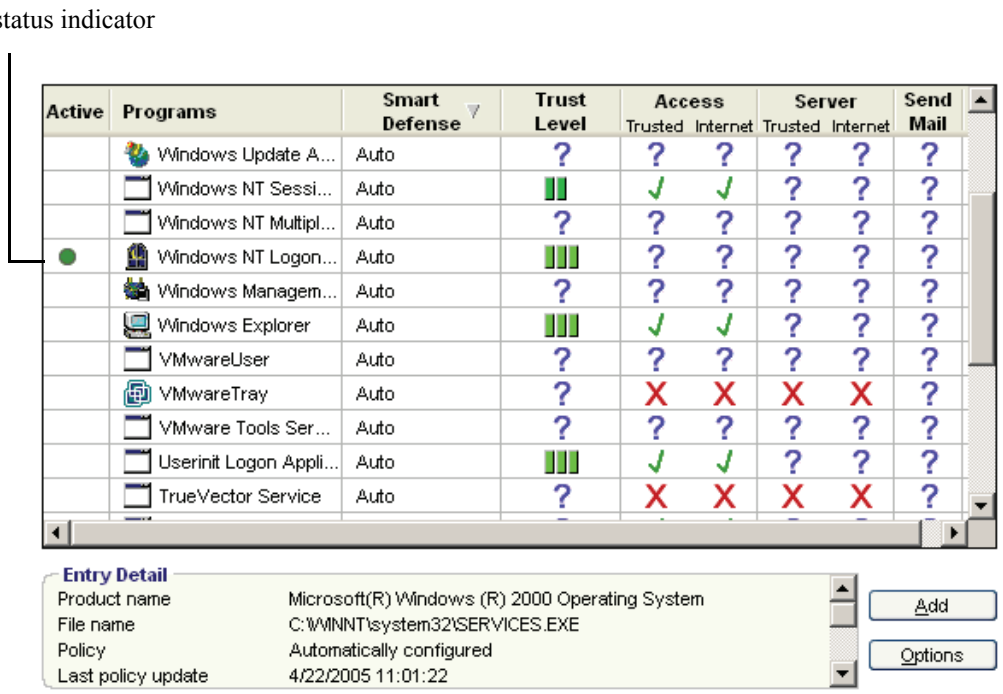


Figure 5-3: Programs list

Active

Indicates the current status of a program. A green circle indicates that the program is currently running.

Programs

The name of the program.

SmartDefense Advisor

The SmartDefense Advisor column indicates where the program policy comes from. The column may contain any of the following designations:

- **Auto**—SmartDefense Advisor determines the program policy, unless a recommendation is not available. (Note that, if SmartDefense Advisor is turned on, and you select **Remember this setting** when responding to a Program alert, the SmartDefense Advisor column will still say Auto, since the permissions will change to conform to any SmartDefense Advisor recommendations that come out later.)
- **Custom**—You determined the program policy manually. If you change a program's permissions (by changing a value in any of the columns in the program's row, for example), the SmartDefense Advisor column displays "Custom" for that program.

- **System**—SmartDefense Advisor determines the program policy, and the program is used by your operating system.

Manually changing the policy for "System" programs could interfere with the normal functions of your computer.

Trust Level

The Trust Level determines the actions that a program is allowed to perform. The Trust Levels are Super, Trusted, Restricted, Ask, Kill, and No Enforcement.

A program's Trust Level setting is determined by its policy. ZoneAlarm security software assigns policies to known programs automatically. The SmartDefense Advisor security team constantly monitors programs for changes in behavior and trustworthiness and updates the programs permissions accordingly. A program with a Trust Level setting of Super today, might have a Trust Level of Restricted tomorrow, if security experts determine that the program could pose a risk to your computer. If you change a program's policy setting from Auto to Custom, however, it will no longer be monitored for changes in Trust Level. For this reason, it is recommended that you keep the default settings for your programs. Refer to the table below for a description the symbols used in this list.

Access

The Access column refers to a program's right to retrieve information from the Internet or networks in the Trusted Zone.

Server

Allows a program to passively listen for contact from the Internet or network. Few programs require server rights.

Send Mail
Allows a program to send and receive e-mail.

Refer to the table below for a description of the symbols used in this list.

Symbol	Meaning
	The program is currently active.
	The program is allowed access/server rights.
	When this symbol appears in the Access or Server columns, it means that ZoneAlarm security software will display a Program alert when the program asks for access, server rights. When this symbol appears in the Trust Level column, it means that ZoneAlarm security software will display a Suspicious Behavior alert when a program performs actions considered suspicious.
	The program is denied access/server rights.
	Super access. Program can perform suspicious actions without seeking permission. No alerts will be displayed.
	Trusted access. Trusted Programs can perform suspicious actions without seeking permission, but unknown programs must ask for permission.
	Restricted access. Program can perform trusted-level actions but cannot perform suspicious actions.
	No access. Programs marked with the No access (Kill) symbol cannot run.
	No enforcement. Program is not monitored at all and can perform any action whatsoever. This setting can pose a security risk.

Table 5-4: Program List symbols

For more information about what program actions are considered suspicious, see "OSFirewall alerts," on page 75.

Adding a program to the programs list

If you want to specify access or server permission for a program that does not appear on the programs list, you can add the program to the list and then grant the appropriate permissions.

To add a program to the programs list:

1. Select **Program Control**|**Programs**, then click **Add**.
2. In the dialog that appears, locate the program you want to add, then click **Open**.

   Be sure to select the program's executable file (for example, program.exe).

To edit a program on the programs list:

1. Select **Program Control**|**Programs**.
2. Right-click a program in the Programs column and choose one of the available options.

Changes Frequently	If this option is selected, ZoneAlarm security software will use only file path information to authenticate the program. The MD5 signature will not be checked. **Caution:** This is a Low security setting.
Options	Opens the Program Options dialog box, in which you can customize security options and create expert rules for programs.
Properties	Opens your operating system's properties dialog box for the program.
Remove	Deletes the program from the list.

Granting a program permission to access the Internet

Many of your most commonly used programs can be automatically configured for safe Internet access. To determine whether a program was configured manually or automatically, select the program in the Programs List and refer to the Policy field in the Entry Details area.

To grant a program permission to access the Internet:

1. Select **Program Control**|**Programs**.
2. In the Programs column, click the program for which you want to grant access, then select **Allow** from the shortcut menu.

For information about granting programs permission by responding to an alert, see "New Program alert," on page 68.

Built-in rules ensure a consistent security policy for each program. Programs with access to the Internet Zone also have access to the Trusted Zone, and programs with server permission in a Zone also have access permission for that Zone. This is why (for example) selecting Allow under Trusted Zone/Server automatically sets all of the program's other permissions to Allow.

Granting a program permission to act as a server

Exercise caution when granting permission for programs to act as a server, as Trojan horses and other types of malware often need server rights in order to do mischief.

Permission to act as a server should be reserved for programs you know and trust, and that need server permission to operate properly.

To grant a program permission to act as a server:

1. Select **Program Control**|**Programs**.
2. In the Programs column, click the program for which you want to grant server access, then select **Allow** from the shortcut menu.

Granting send mail permission to a program

To enable your e-mail program to send e-mail messages and to enable protection against e-mail threats, grant send mail permission to your e-mail program. For more information about protecting your e-mail, see Chapter 9, "E-mail protection," starting on page 147.

To grant send mail permission to a program:

1. Select **Program Control**|**Programs**.
2. Select a program from the list, then click in the **Send Mail** column.
3. Select **Allow** from the shortcut menu.

You also can access the Program Options dialog by right-clicking a program name and selecting **Options**.

Setting program options for a specific program

How a program is authenticated, whether it uses Outbound MailSafe protection, or is held to privacy standards, is determined globally by setting the Program Control level. You can modify these and other settings on a per-program basis from the Programs List.

- Setting Advanced Program Control options
- Disabling Outbound Mail protection for a program
- Setting Filter options for a program
- Setting authentication options
- Setting passlock permission for a program

Setting Advanced Program Control options

Advanced Program Control tightens your security by preventing unknown programs from using trusted programs to access the Internet, or preventing hackers from using the Windows CreateProcess and OpenProcess functions to manipulate your computer.

To enable Advanced Program Control for a program:

1. Select **Program Control**|**Programs**.
2. In the Programs column, select a program, then click **Options**.

   The Program Options dialog appears.
3. Select the **Security panel**, then choose your Advanced Program Control options.

This program may use other programs to access the Internet	Allows the selected program to use other programs to access the Internet.
Allow Application Interaction	Allows the selected program to use OpenProcess and CreateProcess functions on your computer.

4. Click **OK**.

Disabling Outbound Mail protection for a program

By default, Outbound Mail protection is enabled for all programs. Because the ability to send e-mail is not a characteristic of all programs, you may choose to disable Outbound Mail protection for any program that does not require it.

To disable Outbound Mail protection for a program:

1. Select **Program Control**|**Programs**.
2. Select a program from the list, then click **Options**.

   The Program Options dialog appears.
3. Select the **Security** panel.
4. Clear the check box labeled **Enable Outbound MailSafe Protection for this program**.

This check box will not appear unless the SendMail permission for this program is set to Allow.

5. Click **Apply** to save your changes, then click **OK**.

For more information about Outbound MailSafe Protection, see "Outbound MailSafe protection," on page 148.

Setting Filter options for a program

When Parental Control features are enabled globally, individual programs like Word Processing programs can still access restricted content unless filter options have also been enabled for that program. For example, although Parental Control blocks access to the site "http://www.playboy.com" from your browser, the site could still be accessed by clicking a URL within a Microsoft Word document unless Parental Control was also enabled for that program.

To enable filter options for a program:

1. Select **Program Control**|**Programs**.
2. Select a program from the list, then click **Options**.

   The Program Options dialog appears.
3. Select the **Security** panel.
4. Under Filter Options, select the check box beside the protection you want, then click **OK**.

For more information about Parental Control, see Chapter 8, "Parental Controls," starting on page 139.

Setting authentication options

You can specify whether a program is authenticated by using its full pathname or by its components. By default, all programs are authenticated by their components.

To specify an authentication method:

1. Select **Program Control**|**Programs**.
2. Select a program from the list, then click **Options**.

   The Program Options dialog appears.
3. Select the **Security** panel.
4. Under Authentication, select the check box beside the option you want, then click **OK**.

Setting passlock permission for a program

When the Internet Lock is engaged, programs given passlock permission can continue to access the Internet. If you grant passlock permission to a program, and that program uses other applications to perform its functions (for example, services.exe), be sure to give those other programs passlock permission as well.

To grant or revoke passlock permission:

1. Select **Program Control**|**Programs**.
2. Select a program from the list, then click **Options**.

3. Select the **Enable Pass Lock** check box.
4. Click **Apply**, then click **OK**.

Managing program components

In addition to controlling permissions for all *programs* on a computer, advanced users may also want to monitor and, if desired, restrict individual *components* that these programs load (such as DLL files or ActiveX controls). ZoneAlarm security software keeps a list of components (used by allowed programs) that have tried to access the Internet or the local network. Depending on your program control and component control settings, ZoneAlarm security software can simply monitor components or it can alert you each time a new component attempts access. This section explains how to access the Components List and how to change component permissions. For details about enabling component control, see "Enabling Component Control," on page 97.

The Components List contains a list of program components for allowed programs that have tried to access the Internet or the local network. The Access column indicates whether the component is always allowed access, or whether ZoneAlarm security software should alert you when that component requests access. By default, the

Components List is organized in alphabetical order, but you can sort the components in the list by any column by clicking on the Component column header.

To access the Components List:

Select **Program Control** | **Components**.

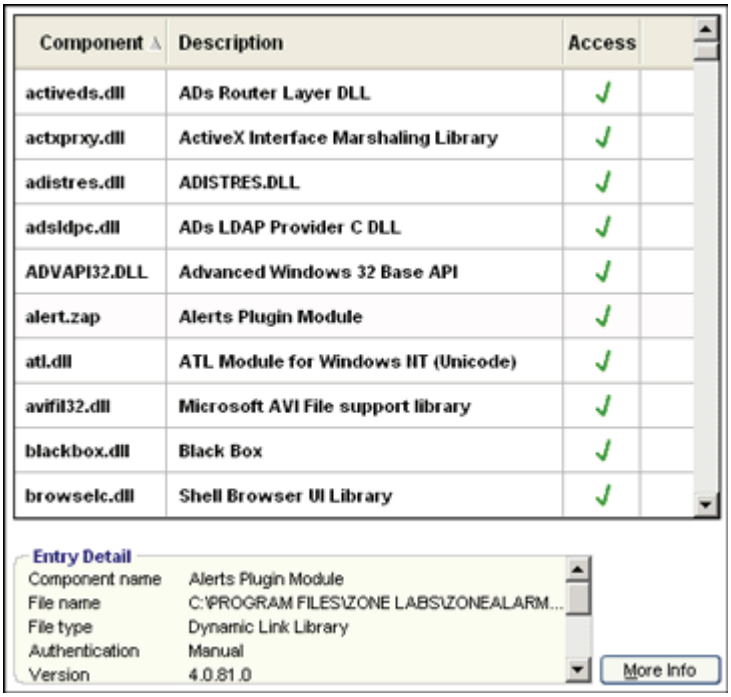


Figure 5-5: Components List

To grant access permission to a program component:

1. Select **Program Control**|**Components**.
2. Select a component from the list, then click in the Access column.
3. Select **Allow** from the shortcut menu.

Creating expert rules for programs

By default, programs given access permission or server permission can use any port or protocol, and contact any IP address or host at any time. Conversely, programs that you block have no access rights at all. By creating expert rules for particular programs, you can heighten protection against hijacked programs by specifying ports and protocols, source and destination addresses, and time and day ranges during which activity is either allowed or denied. You can also apply tracking options to specific types of traffic in

order to see alerts or generate log entries when allowed program traffic occurs, enable or disable rules at will, and apply multiple, ranked rules to a program.

If you created port rules for Programs in a version of ZoneAlarm security software, prior to 4.0, those port rules will be automatically converted to expert rules and visible in the Expert panel of the Program Options dialog. To access the Expert panel, select **Program Control**|**Programs**, then click **Options**.

Creating an expert rule for a Program

Sharing expert rules

Creating an expert rule for a Program

Expert rules for programs are enforced in the order they are ranked. Therefore, when you create expert rules for a program, make sure that the last rule you create for that program is a "Block All" rule.

For tips on setting up expert rules for your programs, visit the ZoneAlarm User Forum (http://www.zonealarm.com/forum) and search for "program rules".

To create an expert rule for a program:

1. Select **Program Control**|**Programs**, then click **Options**.
2. Select **Expert Rules**, then click **Add**.

   The Add rule dialog appears.
3. Create Expert Program rule.

The Add rule dialog contains the same fields and options that are available when you create Expert Firewall rules. Note, however, that IGMP and Custom protocols cannot be applied to expert rules for Programs. See "Creating expert firewall rules," on page 48.

4. Click **OK**.

Sharing expert rules

Expert firewall rules (created in the Firewall | Expert panel) cannot be directly applied to a single program. If the rule is enabled, it is applied globally. Similarly, an expert rule you created for one program cannot be directly applied to another program.

However, you can create a copy of the existing expert rule and apply it to any program. Note that none of the changes you make to the copy will be reflected in the original.

To apply an existing expert firewall rule to a program:

1. Select **Firewall**|**Expert**.
2. Select the rule you want to apply, then press **CTRL**+**C**.
3. Select **Program Control**|**Programs**.
4. In the Programs column, select the program to which you want to apply the expert rule, then click **Options**.
5. Select Expert Rules, then press **CTRL**+**V**.

   The Expert rule is applied to the program.
6. Click **Apply**, then click **OK**.

To disable an Expert rule:

1. Select **Program Control**|**Programs**.
2. Select the program for which you want to disable an Expert Program rule, then right-click and select **Disable** from the shortcut menu.

   The rule will be grayed-out.
3. Click **Apply**, then click **OK**.

Chapter 6

ZoneAlarm browser security

ZoneAlarm adds a toolbar to your browser that protects your computer and your personal data and privacy while you are on the Web.

Topics:

- "Using ZoneAlarm browser security," on page 117

Using ZoneAlarm browser security

The ZoneAlarm browser security toolbar* adds the following important protections.

- Warns you when you go to sites that do not have adequate security credentials.
- Detects known and unknown phishing Web sites.
- When ***virtualization*** is enabled, it can stop malicious zero day drive-by downloads, meaning malware that is not yet known by anti-virus and anti-spyware engines and has no known solution. (Not included in some versions.)**
- Lets you choose a Privacy Browser option when you want to leave no trace on your computer of what you've typed or where you've been. (Not included in some versions.)**
- Checks anything you download from the Web for malware, using a sophisticated multi-layer scanning process. (Not included in some versions.)**
- Blocks the processes that keylogger and screen grabber malware use to secretly record your keystrokes or onscreen activity. This helps ensure that even keyloggers or screen

grabbers that have not yet been discovered are rendered harmless. (Not included in some versions.)**

See the Help provided in the ZoneAlarm browser toolbar for full details.

*Also called ForceField in some versions.

**See www.zonealarm.com/featurehistory to find out which features are included each product.

Turning virtualization on

Virtualization may not be on by default in your version of the software. (Not included in some versions. You can upgrade to include this protection.)

Virtualization is the feature that can stop dangerous drive-by downloads—even ones that are not yet known by anti-virus and anti-spyware engines.

To enable virtualization:

1. Select **Browser Security**|**ForceField**.
2. Click the **Settings** button.
3. Select **Enable virtualization**.

Turning browser security on and off

ZoneAlarm browser security performs much of its work behind the scenes, until it needs to warn you about a danger or let you know the results of a download scan. You know that ZoneAlarm browser security is on you when you see the ZoneAlarm toolbar in your browser. Also, a faded white edge appears around your browser (except when browser window is maximized).

To turn browser security or off from ZoneAlarm:

1. Select **Browser Security.**
2. Click **On** or **Off**.

To turn browser security on or off from your browser:

1. In your browser window, choose **View | Toolbars**, and then select or deselect "Browser security toolbar" or "Forcefield security toolbar."
2. Restart your browser.

Accessing ZoneAlarm browser security Help and troubleshooting

1. With ZoneAlarm browser security enabled, open a Web browser.
2. From the **ZoneAlarm browser toolbar menu**, choose **Help**.

Chapter 7

Virus and spyware protection

The integrated antivirus and anti-spyware feature protects your computer against viruses and spyware in a single powerful operation. Multiple scanning options automatically detect viruses and spyware and render them harmless before they can damage your computer.

Topics:

- "Spyware and virus Protection," on page 120
- "Customizing virus protection options," on page 122
- "Performing a scan," on page 129
- "Viewing virus and spyware protection status," on page 135
- "Monitoring virus protection," on page 136

Spyware and virus Protection

The anti-virus/anti-spyware engine keeps known and unknown malware from affecting your computer by scanning files and comparing them to a database of known malware and against a set of characteristics and patterns (heuristics) that reflect malware behavior. Files can be scanned as they are opened, closed, executed, or as part of a full computer-wide scan. If a virus is detected, ZoneAlarm security software renders it harmless, either by repairing or denying access to the infected file.

- Turning on virus and spyware protection
- Scheduling regular scans
- Keeping virus definitions up-to-date

Turning on virus and spyware protection

If you chose not to turn on the anti-virus protection feature in the Configuration Wizard following installation, you can turn it on manually.

The ZoneAlarm Anti-virus protection feature is incompatible with other virus protection software. Before you turn on the Anti-virus protection feature, you must uninstall any other anti-virus software from your computer, including suite products that include virus protection among their features.

To enable virus and spyware protection:

1. Select **Anti-virus/spyware**.
2. On **Anti-virus/spyware** panel, select **On**.

Scheduling regular scans

By default, a system malware scan is performed once per week. You can customize the time and frequency. Scanning your computer for viruses and spyware is one of the most important things you can do to protect the integrity of your data and computing environment.

If your computer is not on when the scheduled scan is set to occur, the scan will occur fifteen minutes after your computer is restarted.

To schedule a scan:

1. Select **Anti-virus/spyware**.
2. Click **Advanced Options**.
3. Under Advanced Settings, select **Scan Schedule**.
4. Select the **Scan for viruses** check box, then specify a day and time for the scan.
5. Specify the scan frequency.
6. Click **OK**.

Keeping virus definitions up-to-date

Every virus or spyware application contains unique identification information, known as its signature definition file. These files are the maps used to locate viruses and spyware on your computer. As new viruses or spyware applications are discovered, ZoneAlarm security software updates its databases with the signature definition files it needs to detect these new threats.

Therefore, your computer is vulnerable to viruses and spyware whenever its database of virus definitions files becomes outdated. But, do not worry:

- By default, the signature files are automatically updated frequently.

- If you hear of an outbreak and want to get the latest updates immediately, click **Check for Updates** under **QuickTasks** in the ZoneAlarm window.

This panel displays the Update status of your signature files.

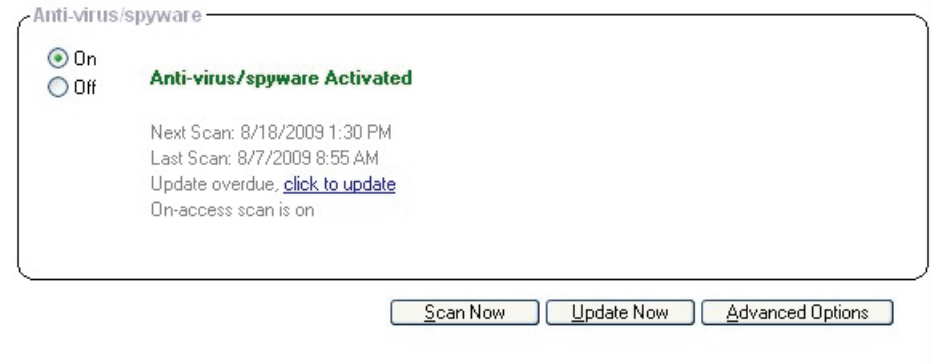


Figure 7-1: Anti-virus/spyware status

By leaving the automatic update feature on, you will always receive the latest signature files when they are available.

To customize automatic signature updates:

1. Click the **Advanced Options** button.
2. Select **Updates**, then:
   - Select the **Enable automatic anti-virus updates** check box.
   - Adjust the **update frequency** if you want updates more or less often.
3. Click **OK**.

Customizing virus protection options

In addition to choosing the type of scan you want to perform, you also can specify the method used to detect viruses, and set treatment methods.

ZoneAlarm security software provides several types of virus scans to keep your computer and data safe: system scans, on-access scans, and e-mail scans.

- Specifying scan targets
- Choosing a scan mode
- Configuring on-access scanning
- Enabling automatic virus treatment

- Specifying scan options
- Excluding items from virus scans

Specifying scan targets

You can specify which drives, folders, and files are scanned when a scheduled or manual system scan occurs. Exclude or include an item in the scan by selecting the checkbox beside it. By default, ZoneAlarm security software only scans local hard drives.

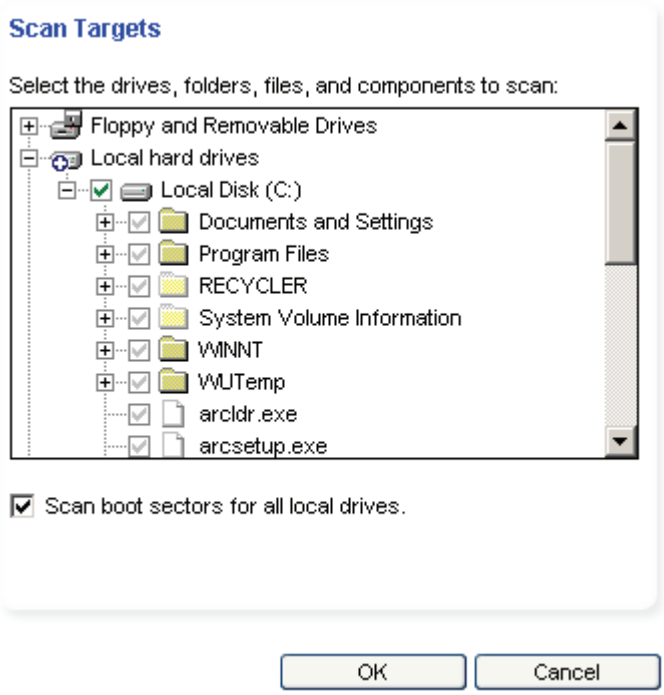


Figure 7-2: Scan targets dialog box

Table 6-2 below provides an explanation of the icons shown in the Scan Targets dialog box.

Icon	Explanation
	The selected disk and all sub-folders and files will be included in the scan.
	The selected disk and all sub-folders and files will be excluded from the scan.
	The selected disk will be included in the scan, but one or more sub-folders or files will be excluded from the scan.
	The selected folder will be excluded from the scan, but one or more sub-folders or files will be included in the scan.

Table 7-3: Icons indicating scan targets

Icon	Explanation
	The selected folder will be included in the scan. A gray check mark indicates that scanning of the folder or file is enabled because scanning has been enabled for a higher level disk or folder.
	The selected folder will be excluded from the scan. A gray "x" mark indicates that scanning of the folder or file is disabled because scanning has been disabled for a higher level disk or folder.

Table 7-3: Icons indicating scan targets

Keep in mind that your Scan Mode settings override your Scan Target settings. For example, regardless of the folders you select as your Scan Targets, if Quick Scan is your Scan Mode then the only folders scanned are Windows and Startup folders. See also "Choosing a scan mode," on page 124.

To specify scan targets:

1. Select **Anti-virus/spyware** and click **Advanced Options**.
2. Under Virus Management, select **Scan Targets**.
3. Select the drives, folders, and files to be scanned.

   The **Other** option listed refers to RAM disks and any unknown drive *other than* floppy, removable, local, remote, CD, and network drives.
4. Select or clear the **scan boot sectors for all local drives** check box.
5. Select or clear the **scan system memory** check box, then click **OK**.

Choosing a scan mode

You can choose one of four different system scan modes, from the most thorough to the fastest. Scan modes apply to the scans that run according to a regular schedule and when you click a Scan button.

For the first system scan after installation, ZoneAlarm uses the Ultra Deep scan mode in order to create a secure baseline. After that, system scans default to the Normal mode, which is faster and skips archive files and other files that are not executable.

Choosing a Scan Mode:

1. Select **Anti-virus/spyware**, and then click the **Advanced Options** button.
2. In the dialog that appears, under **Advanced Options**, click **Scan Mode.**

3. Choose a scan:

Ultra Deep Scan	**Slowest and most thorough.** Scans all files, folders, and archive files (e.g., zipped files). Also includes heuristic scanning to detect malware not yet registered in databases. Note that heuristics that may occasionally result in false positive detections since it detects characteristics rather than signatures.
Deep Scan	**Very thorough**. Recommended every six months or after exposure to a virus outbreak. Scans all files and folders. Skips archive files which pose minimal risk because they cannot self-activate.
Normal Scan	**Fast, default scan**. Recommended as your regular scan mode. By skipping archive and non-executable files you get a quicker scan with minimal risk of missing viruses that could self-activate.
Quick Scan	**Fastest**. Scans only Windows folders, Startup folders, and folders linked to startup items, which are common places for hackers to place viruses. (Programs in these folders can run automatically without permission, which creates the most risk.)

Keep in mind that your Scan Mode settings override your Scan Target settings. For example, regardless of the folders you select as your Scan Targets, if Quick Scan is your scan mode the only folders scanned are Windows and startup folders.

Configuring on-access scanning

On-access scanning protects your computer from viruses by detecting and treating viruses that may be dormant on your computer. It is on by default and supplies the most active form of malware protection, so we recommend you keep it enabled.

Files are scanned for viruses as they are opened, executed, or saved, thereby allowing immediate detection and treatment of viruses.

Archive files, such as .zip files, are scanned by on-access scanning when you open them. In Ultra Deep Scan mode, archive files will also be scanned by system scans.

To enable on-access scanning:

1. Select **Anti-virus/spyware**.
2. In the Protection area, click **Advanced Options**.

3. Under Advanced Settings, select **On-Access Scanning**.
4. Select **Enable On-Access Scanning**, and optionally specify a mode, then click **OK**:

Scan in Smart Mode	(Recommended) Scans files when they are opened, saved, or executed, and expedites this process by leveraging information from previous scans.
Scan when reading	Scans a file when it's opened or executed.
Scan when reading and writing	Scans a file when it's opened, saved, or executed.

Enabling on-access scanning of network files

You can enable on-access virus/spyware scanning of the files that exist on any drives or computers you are connected to on a network. Note that this option may not be necessary, and may slow performance, if these drives already have full security protection.

1. On the Antivirus/spyware panel, click **Advanced Options**.
2. Select **On-Access Scanning**.
3. Select **Enable scanning of network files**.

Enabling automatic virus treatment

By default, ZoneAlarm security software automatically attempts to treat files that contain viruses. If a file cannot be repaired, the Scan Results dialog will inform you so that you can take the appropriate action. When a virus infection is detected, the Scan Results dialog offers the available treatment options, such as Quarantine, Repair, or Delete.

To enable automatic virus treatment:

1. Select **Anti-virus/spyware**, then click **Advanced Options**.
2. Under Virus Management, select **Automatic Treatment**.
3. Select the auto treatment option you want:

▪	Alert me - do not treat automatically
▪	Try to repair, and alert me if repair fails
▪	Try to repair, quarantine if repair fails (recommended)

4. Click **OK**.

Specifying scan options

These options apply to on-demand scans and on-access scans. These options do not apply to contextual (i.e., select item and right-click) scans.

To specify virus scan options:

1. Select **Anti-virus/spyware**, then click **Advanced Options**.
2. Under **Virus Management**, select **Scan Options**.
3. Select your desired settings, then click **OK**.

Skip if the object is greater than	This option improves scan time without increasing risk, as virus files are usually smaller than 8 MB. While large files ignored by the scan may contain viruses, these viruses can still be caught by on-access scanning, assuming you have on-access enabled. Enter a maximum object size in the **MB** field.
Enable riskware* scanning	Warns you about programs that could potentially be a security risk if accessed or controlled by hackers. Riskware includes common programs, such as chat and web downloader programs, that are known to have security vulnerabilities. They be used to cause damage or steal information. When riskware is detected, ZoneAlarm asks your permission to let it run.*
Enable cpChecker	Optimizes performance by minimizing scanning according to rules that leverage prior scan data. Works on limited file sizes and formats. Most efficient when cpSwift is also enabled.
Enable cpSwift	Optimizes performance by minimizing scanning according to rules that leverage prior scan data. Works on any file formats, sizes, and types. Most efficient when cpChecker is also enabled.
Enable ADS scanning	Scans alternative data streams (ADS), which can sometimes hide malware in otherwise benign files.
Enable heuristics scanning	Scans files for specific information or characteristics associated with malware. Adds another layer of security by detecting viruses or spyware not yet known to virus signature databases.

***Other programs that may be detected as riskware include:** remote administration programs, FTP servers, proxy servers, password recovery tools, monitoring programs, automatic dialing programs, telnet servers, Web servers, computer tools, network tools, peer-to-peer client programs, SMTP clients, Web toolbars, and known fraudulent programs. Of these types of programs, only those known for security vulnerabilities will be detected as riskware.

Excluding items from virus scans

Excluding items from virus scans can be useful in the following circumstances:

- When you don't want ZoneAlarm to scan certain directories, files, or programs that you know to be safe, see "Excluding files from virus scans," on page 128.
- If a scan reports as a virus a program you know to be safe, see "Excluding detected viruses from scans," on page 128.

Excluding files from virus scans

You may want to exclude certain files and programs you know to be safe.

To specify items that should be ignored by virus scans:

1. Select **Anti-virus/spyware**, then click **Advanced Options**.
2. Under Virus Management, select **Exceptions**.
3. Click the **Add File** button and choose from the **Select type** menu:

On-Access scan	Excludes the selected file(s) from on-access scans, which occur when a file is opened, executed, or saved.
Trusted Process	Choose this if you want to exclude an executable (.exe) file from scans.

4. Do one of the following:
   - Click **Browse** to select a file you want to exclude.
   - To exclude a drive or group of files, enter them into the **Select exception** field using one of the formats shown in the Browse dialog box.
5. Click **OK**.

Excluding detected viruses from scans

Some benign applications may be mistaken as viruses during a system or on-access scan. If an application shows up in the Scan Results but you are certain it is safe, you can exclude it from anti-virus scans by adding it to the exceptions list.

To exclude a suspected virus from future scans:

- When a virus **Scan Results** dialog appears, right-click programs that you want to exclude and choose **Ignore Always**.

The program is added to exceptions list and will no longer be detected during virus scans.

Performing a scan

There are several ways you can run anti-virus/spyware scans on your computer. Once a scan starts, a dialog appears from which you can pause or cancel the scan if you want to.

Scan	How to run it
On-demand (manual) system scan	Under **Quick Tasks**: Click **Scan Computer**. Or, from the Anti-virus/spyware panel: Click **Scan Now** button.
Scheduled system scan	System scans are set to run regularly by default. You can set how often they run. See "Scheduling regular scans," on page 121.
Contextual scan (manual file scan	To instantly scan a specific file, right-click the file, then choose **Scan with ZoneAlarm Anti-virus**.
On-access scan	Open a file—the file is instantly scanned in the background upon opening. On-access scanning is enabled by default. See "Configuring on-access scanning," on page 125.

Table 7-4: How to perform different types of scans

You may run up to five scans simultaneously. Scans are performed in the order in which they are initiated. System scans provide another level of protection by allowing you to scan the entire contents of your computer at one time. System scans detect viruses that may be dormant on your computer's hard drive, and if run frequently, can ensure that your anti-virus signature files are up to date.

Because of the thorough nature of full-system scans, some can take a while to perform. To avoid any impact on your workflow, you can schedule system scans to run at a time when you are least likely to be using your computer.

Tip: You can customize your system scans. Choose from these scan modes: Ultra Deep, Deep, Normal, or Quick. See "Choosing a scan mode," on page 124.

During scans, ZoneAlarm security software displays a special system tray icon ( ) and provides a system tray menu option for viewing scan status. Right-click the system tray icon and choose **View Scan** to check on scan status.

Clicking **Pause** in the Scan dialog while a scan is being performed will stop the current scan only. On-access scanning will not be disabled. Click **Pause** again to resume the current scan.

- .Understanding virus scan results
- Treating virus files manually

- Repairing files in an archive
- Submitting viruses and spyware to ZoneAlarm for review
- Viewing logged virus events
- Viewing items in quarantine

Understanding virus scan results

Regardless of the method used to initiate the scan, the results of the scan are displayed in the Scan Results dialog box as shown
below

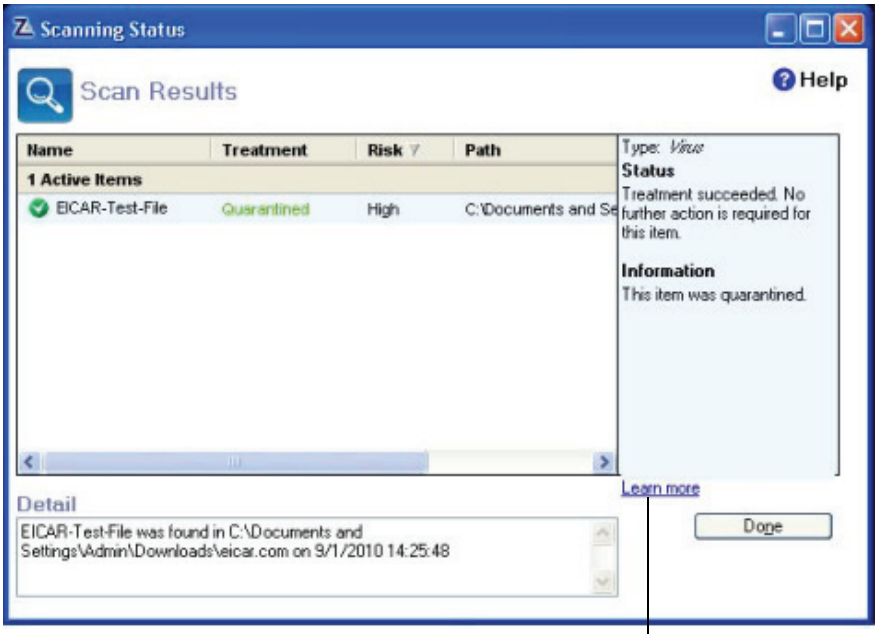


Figure 7-5: Scan results dialog

The Active Items area of the Scan details dialog lists infections found during the scan that could not be treated automatically. To accept the suggested treatments in the Treatment column, click **Apply**. The items listed under Auto Treatment have already been treated, you do not need to take further action.

If the scan results list any programs that you are certain are safe (not viruses), you can exclude it from future scans. See "Excluding detected viruses from scans," on page 128

Name
The name of the virus that caused the infection.

Treatment
Specifies the treatment applied to the infection. Possible values are Quarantined or Deleted.

Security Risk
Indicates the risk level of the infection. All viruses are considered High risk.

Path
The location of the virus that caused the infection.

Type
Specifies whether the infection was caused by a virus, worm, or trojan.

Status
Tells you whether the file has been repaired, deleted, or remains infected. If ZoneAlarm security software was unable to treat the item, a **What to do next** link may appear here. This link will direct you to further information and instructions.

Information
Provides more detail about the infection. To get more information about a virus or spyware, click the **Learn more** link.

Detail
Lists the location of virus traces. Advanced users may find this information useful for tracking down viruses that cannot be treated automatically.

Treating virus files manually

If you do not have automatic treatment enabled, or if a file could not be repaired automatically, you can attempt to treat it manually from the Scan Results dialog.

To treat a file manually:

1. In the Scan Results dialog, select the item you want to treat.
2. In the Treatment column, choose the treatment option you want:

Repair	Tries to repair the selected file.
Delete	Deletes the selected file.
Quarantine	Appends the extension .zl6 to the infected file to render it harmless. The file is placed in Quarantine.

3. When you have finished treating files, click **Close**.

If the results of a virus scan contain Error, No treatment available, or Treatment failed, it means that there is not yet a way to automatically remove the virus without risking the integrity of your computer or other files. In some cases, there may be manual treatments available to you. To find out, enter the name of the virus along with the word "removal" into a search engine, such as Google or Yahoo, to locate removal instructions. Otherwise, know that we're constantly researching viruses and developing safe ways to remove them.

Repairing files in an archive

If the infected file is located in an archive file (such as a .zip file), ZoneAlarm security software will not be able to treat it (either by repairing, deleting, or placing it in Quarantine) while the file is still included in the archive.

To repair a file in an archive:

1. Select **Anti-virus/spyware**, then click **Advanced Options**.
2. Select **On-Access Scanning**, then select the **Enable On-Access Scanning** check box.
3. Click **Apply**, then click **OK**.
4. Open the file that was specified in the Scan Results dialog from within an archival utility, such as WinZip.

   On-access scanning will scan the file for infections. The Scan Results dialog will appear with the results of the scan. If the file still cannot be repaired, see "Treating virus files manually," on page 131.

Submitting viruses and spyware to ZoneAlarm for review

Reporting and submitting suspected malware to ZoneAlarm, a Check Point Software Technologies, Inc. Company helps to improve the security and protection of all Internet users. The ZoneAlarm Security Team monitors all incoming submissions for new files. The ZoneAlarm Security Team will act on your submission as appropriate and may contact you for more information or to provide details about the files you submit.

Due to the volume of malware released each day, our researchers cannot respond to each file you submit. However, we appreciate the assistance of our users and thank you for taking the time to help secure the Internet. Please address any questions or concerns to: **security@zonealarm.com**

To submit malware to ZoneAlarm for review:

1. Place the malware file in a password-protected .zip archive with the password set to *infected*.

   For help with creating a password protected archive, refer to the Help for WinZip.

2. Send the .zip file to malware@zonealarm.com

   Use this e-mail address only for sending malware to the ZoneAlarm Security Team.

Please do not send malware files if you feel you cannot do so safely or if it would increase the risk of infection or damage to your system. Do not e-mail suspected malware files to others as they could be malicious.

Viewing logged virus events

By default, all Virus events are recorded in the Log Viewer.

To view logged Virus events:

1. Select **Alerts & Logs | Log Viewer**.
2. Select **Virus**, from the Alert Type drop-down list.

Table 6-3 provides an explanation of the log viewer fields available for Virus events.

Field	Information
Date	The date of the infection.
Type	The type of event that occurred. Possible values for this field include: • Update • Scan • Treatment • E-mail
Virus name	The common name of the virus. For example, *iloveyou.exe*.
Filename	The name of the infected file, the name of files being scanned, or the name and version number of update and/or engine.

Table 7-6: Virus event log fields

Field	Information
Action Taken	How the traffic was handled by ZoneAlarm security software. Possible values include: • Updated, Update cancelled, Update Failed • Scanned, Scan cancelled, Scan Failed • File Repaired, File Repair Failed • Quarantined, Quarantine Failed • Deleted, Delete Failed • Restored, Restore Failed • Renamed, Rename Failed
Actor	Whether the action was manual or auto.
E-mail	If the virus was detected in e-mail, the e-mail address of sender of the infected message.

Table 7-6: Virus event log fields

Viewing items in quarantine

In some cases, items detected during a virus or spyware scan cannot be treated or removed automatically. These items are usually placed into quarantine so that they are rendered harmless but preserved so that they may be treated in the future after an update to your virus and spyware signature files.

To view viruses in quarantine:

1. Select **Anti-Anti-virus / Anti-spyware** | **Quarantine**.
2. Choose **Viruses** from the Quarantined View drop-down list.
3. Optionally, select a virus entry in the list and click **Delete** (to delete it from your computer), **Restore** (to restore it to your computer), or **More Info** (to consult SmartDefense Advisor for more information about it).

The virus view in quarantine contains the following columns of information:

Infection
The name of the virus that caused the infection.

Days in Quarantine
The number of days the virus has been in quarantine.

Path
The location of the virus on your computer.

To view spyware in quarantine:

1. Select **Anti-virus / Anti-spyware** | **Quarantine.**

2. Choose **Spyware** from the Quarantined View drop-down list.
3. Optionally, select a spyware entry in the list and click **Delete** (to delete it from your computer), **Restore** (to restore it to your computer), or **More Info** (to consult SmartDefense Advisor for more information about it).

The spyware view in quarantine contains the following columns of information:

Type
The name of the virus that caused the infection.

Name
The name of the spyware that was detected.

Risk
The risk level of the infection. Indicates whether the spyware is benign like adware, or a serious threat like keylogging software.

Days in Quarantine
The number of days the spyware has been in quarantine.

Viewing virus and spyware protection status

The **Anti-virus/spyware** panel displays the status of your virus and spyware protection. From this area you can:

- Verify that virus and spyware protection is turned on.
- The dates and times of your last scan(s).
- Update definition files.
- Invoke a scan.
- View results of latest scan.
- Access advanced settings.

The section that follows describes the status information located on the main panel of the Anti-virus / spyware panel.

- Monitoring virus protection
- Enabling and disabling Anti-virus Monitoring
- Viewing Status Messages in the Anti-virus Monitoring panel
- Performing a scan

Monitoring virus protection

One of the most important things you can do to protect your computer against viruses is to install an anti-virus software product. Once installed, however, the anti-virus software must be kept up to date to ensure protection against new viruses as they are created.

No matter which anti-virus software product you use, if you find yourself in either of the following situations, you are putting your computer at risk for virus attack:

- Your trial or subscription period has expired.
- Your virus signature files are out of date.

Anti-virus Monitoring is a secondary defense system that tracks anti-virus software you have installed on your computer and lets you know when that anti-virus software is out-of-date or turned off. This secondary alerting system works as a back-up to your anti-virus software's built-in warning and update system. Most anti-virus products include automatic updating, and alert you when your virus definition files become outdated. Note that not all anti-virus products are supported by this feature.

- Monitoring Coverage
- Monitoring product status
- Monitoring antivirus status alerts
- Enabling and disabling Anti-virus Monitoring
- Viewing Status Messages in the Anti-virus Monitoring panel
- Monitoring antivirus status alerts

Monitoring Coverage

Anti-virus Monitoring currently detects anti-virus software from these popular manufacturers:

- Symantec
- McAfee
- Computer Associates
- Trend Micro

If you use a different anti-virus product, Anti-virus Monitoring will not recognize it at this time. This does not mean that your ZoneAlarm product is malfunctioning; your security remains as strong as ever. ZoneAlarm security software will be adding the ability to recognize more products over time. If your anti-virus product is not currently supported, you may simply turn off the Anti-virus Monitoring feature. Do not worry--Anti-virus Monitoring is monitoring only and has no affect on the firewall and no direct affect on security.

Monitoring product status

In these products, you will see an Anti-virus Monitoring panel. From this panel you can view the status of your anti-virus product. You can also turn monitoring on or off, or you can turn on or off just the monitoring alerts.

To turn off Monitoring and Monitoring alerts:

1. Select **Anti-virus Monitoring**.
2. In the **Monitoring** area, select **Off**.
3. Clear the check box **Notify me of anti-virus security lapses**.

Monitoring antivirus status alerts

In products where there is no Anti-virus Monitoring panel because the products are equipped with ZoneAlarm Anti-virus, there are monitoring alerts. When ZoneAlarm Anti-virus is turned off, the Anti-virus Monitoring feature is activated. Monitoring can be turned off from any monitoring alert, or from the Advanced Options dialog.

To turn off Monitoring

1. Select **Alerts & Logs | Main**, then click **Advanced**.
2. Select the **Alerts Events** panel.
3. Clear the following check boxes:

▪	Anti-virus protection not found
▪	Anti-virus events

4. Click **OK**.

Enabling and disabling Anti-virus Monitoring

If you do not have ZoneAlarm Anti-virus installed and are using another anti-virus software product, Anti-virus Monitoring will be enabled by default. In addition, you can choose to enable Monitoring alerts, which will appear whenever a lapse in protection is detected.

To enable or disable Anti-virus Monitoring:

1. Select **Anti-virus Monitoring**.
2. In the Anti-virus Monitoring area, select **On**.

Viewing Status Messages in the Anti-virus Monitoring panel

The Status area of the Anti-virus Monitoring panel displays the current state of your installed Anti-virus products, as well as the state of Anti-virus Monitoring.

Chapter 8

Parental Controls

Parental Controls protect your family from Web sites containing content you do not want them to access. You can choose which categories of Web sites to block, and use Smart Filtering to instantly categorize and filter previously un-rated sites.

Topics:

- "Using Parental Controls," on page 139
- "Choosing which content categories to block," on page 141

Using Parental Controls

When your browser is pointed to a Web site or other Web-based content, ZoneAlarm security software contacts *Blue Coat*™ Parental Controls servers to see how that site or content has been categorized. If the site your browser is trying to reach has been placed by Blue Coat ™ in a category you have decided to block, access to the site is denied. This process normally takes less than a second. A Parental Control Violation page is displayed, explaining why the site was blocked. If you disagree with a site categorization, you can request a reevaluation of the site by clicking a link in the Filtering Violation page that appears when the site is blocked.

- Working with parental controls and smart filtering
- Choosing which content categories to block

Working with parental controls and smart filtering

When you enable Parental Controls, you immediately block Web sites that Blue Coat has determined contain nudity, pornography, information on illegal drugs, racist text or images,

and other content you might not want your children exposed to. If you enable Smart Filtering, new and nonrated sites will instantly be categorized and filtered, enhancing your protection.

To prevent your children from changing your Parental Controls settings, set a ZoneAlarm security software password. See "Setting your password," on page 14.

- Enabling or disabling Parental Controls
- Enabling or disabling Smart Filtering
- Setting timeout options

Enabling or disabling Parental Controls

The Parental Controls let you block sites that are set to Block in the Categories List. If Parental Controls are disabled, Category and Smart Filtering settings are ignored.

To enable or disable Parental Controls:

1. Select **Parental Controls | Main**.
2. In the Parental Controls area, click **On** or **Off**.

Enabling or disabling Smart Filtering

Smart Filtering (Dynamic Real-Time Rating) lets you block undesirable sites even if they are brand-new and have not yet been categorized. When this feature is enabled, and your computer points to uncategorized content, Blue Coat™ instantly analyzes the content of the Web site and places it in a category. The site is then blocked or allowed based on your Parental Controls settings. This process normally takes two to four seconds.

To enable or disable Smart Filtering:

1. Select **Parental Controls | Main.**
2. In the Smart Filtering area, select **On** or **Off**.

   To access this option, Parental Controls must be enabled.

Setting timeout options

Timeout options determine how long ZoneAlarm security software will try to obtain a rating for a Web site, and what it do if it is unable to obtain one.

To set timeout options:

1. Select **Parental Controls | Main**,
2. Click the **Advanced** button.

3. Specify your timeout preferences.

Parental Controls timeout (sec)	The interval, in seconds, for which ZoneAlarm security software will try to obtain a rating when Smart Filtering is disabled.
Timeout when DRTR enabled (sec)	The interval, in seconds, for which ZoneAlarm security software will try to obtain a rating when Smart Filtering is enabled.
When rating unavailable	Specifies whether ZoneAlarm security software should allow or block sites for which a rating is unavailable.

4. Click **OK**.

If **When rating unavailable** is set to **allow the site**, setting the timeout options to very low numbers might cause undesirable sites to be allowed. We recommend keeping the default timeout options.

Choosing which content categories to block

Parental Controls provide numerous categories for filtering Web content. Table 11-1 below provides a description of each category, along with its default setting.

To change the setting for a category:

1. Select **Parental Categories | Main**.
2. In the Site Categories to block column, select or clear the check box beside the category.

   A red check mark indicates that content belonging to that category will be blocked. An empty check box indicates that content belonging to that category will be allowed.

To block all site categories, click **Check All**. To allow all site categories, click **Clear All**. To revert to default settings, click the **Reset to Defaults** link.

Category	Definition	Default Setting
Abortion	Site which provide information or arguments in favor of or against abortion; describes abortion procedures; offers help in obtaining or avoiding abortion; provides information on the physical, social, mental, moral, or emotional effects, or the lack thereof, of abortion.	Allowed

Table 8-1: Parental Control categories

Category	Definition	Default Setting
Adult: Intimate Apparel/Swimsuit	Sites offering pictures of models in lingerie, swim wear or other types of suggestive clothing. This does not include sites selling undergarments as a sub-section of the other products offered.	Allowed
Adult: Nudity	Sites containing nude or semi nude depictions or pictures of the human body. These depictions are not necessarily sexual in intent or effect but may include sites containing nude paintings or photo galleries of artistic nature. It also includes nudist or naturist sites that contain pictures of nude individuals.	Blocked
Adult: Pornography	Sites containing sexually explicit material for the purpose of arousing a sexual or prurient interest.	Blocked
Adult: Sex Education	Sites that provide information on reproduction, sexual development, sexually transmitted disease, contraception, safe sex practices, sexuality and sexual orientation. This does not include sites offering suggestions or tips on how to have better sex.	Allowed
Alcohol/Tobacco	Sites that promote or offer for sale alcohol/tobacco products or provide the means to create them. Also may include sites that glorify, tout or otherwise encourage the consumption of alcohol/tobacco.	Blocked
Chat Room / Instant Messenger	Sites that provide chat and Instant Messaging capability.	Allowed
Criminal Skills / Illegal Skills / Cheating	Sites that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. Sites that provide instructions about or promote crime, unethical/dishonest behavior or evasion of prosecution thereof.	Blocked
Cult / Occult	Prominent organized modern religious groups that are identified as "cults" by three or more authoritative sources. Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers or supernatural beings.	Allowed
Dating and Personals	Sites that promote interpersonal relationships. Does not include those pertaining to gay or lesbian appeal.	Allowed

Table 8-1: Parental Control categories

Category	Definition	Default Setting
Drugs: Illegal Drugs	Sites that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.	Blocked
E-mail	Sites offering Web-based E-mail services.	Allowed
Freeware / Software Downloads	Sites that promote or offer free software or products for general download or trial purposes.	Allowed
Gambling	Sites where a user can place a bet or participate in a betting pool (including lotteries) online; obtain information, assistance or recommendations for placing a bet; receive instructions, assistance or training on participating in games of chance. Does not include sites that sell gambling related products or machines.	Blocked
Gay and Lesbian	Sites that provide information on or cater to gay and lesbian lifestyles. Does not include sites that are sexually oriented.	Allowed
Glamour / Lifestyle	Sites that emphasize or provide information or news on how the user can achieve physical attractiveness, allure, charm, beauty, or style with respect to personal appearance.	Allowed
Government: Military	Sites that promote or provide information on military branches or armed services.	Allowed
Hacking / Proxy Avoidance Systems	Sites providing information on illegal or questionable access to or the use of communications equipment/software, or provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server.	Blocked
Humor / Jokes	Sites that primarily focus on comedy, jokes, fun, etc. Does not include sites containing jokes of adult or mature nature.	Allowed
Internet Auctions	Sites that support the offering and purchasing of goods between individuals.	Allowed
MP3 / Streaming	Sites that support and or allow users to download music and media files such as MP3, MPG, MOV, etc. Also includes sites that provide streaming media (radio, movie, TV).	Allowed
News Groups	Sites that offer access to Usenet New Groups or other like sites.	Allowed

Table 8-1: Parental Control categories

Category	Definition	Default Setting
News and Media	Sites that primarily report, information, or comments, on current events or contemporary issues of the day. Items like weather, editorials, and human interest are considered target within the context of major news sites.	Allowed
Online Games	Sites that provide information and support game playing or downloading, video games, computer games, electronic games, tips and advice on games or how to obtain cheat codes, journals and magazines dedicated to game playing, online games, as well as sites that support or host online games including sweepstakes and giveaways.	Allowed
Pay to Surf Sites	Sites that pay users money for clicking on specific links or locations.	Blocked
Political /Activist / Advocacy	Sites that are sponsored by and contain information about specific political parties or groups. Sites that are sponsored by or devoted to organizations that promote change or reform in public policy, public opinion, social practice, economic activities and relationships. Excludes commercially sponsored sites dedicated to electoral politics or legislation.	Allowed
Religion	Sites that promote and provide information on Buddhism, Baha'I, Christianity, Christian Science, Hinduism, Islam, Judaism, Mormonism, Shinto, Sikhism, Atheism, other conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, other houses of worship, any faith or religious beliefs including “alternative” religions such as Wicca and witchcraft.	Allowed
Search Engines / Portals	Sites that support searching the Web, indices and directories.	Allowed
Shopping	Sites that provide the means to obtain products and services that satisfy human wants and or needs. This does not include products or services that are principally marketed to satisfy industrial or commercial needs.	Allowed
Sports / Recreation / Hobbies	Sites that promote or provide information about spectator sports.	Allowed

Table 8-1: Parental Control categories

Category	Definition	Default Setting
Violence / Hate / Racism	Sites which advocate or provide instructions for causing physical harm to people or property through use of weapons, explosives, pranks, or other types of violence. Sites that advocate hostility or aggression toward an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics; a site which denigrates others on the basis of those characteristics or justifies inequality on the basis of those characteristics; a site which purports to use scientific or other commonly accredited methods to justify said aggression, hostility or denigration.	Blocked
Weapons	Sites that sell, review, or describe weapons such as guns, knives, or martial arts devices, or provide information on their use, accessories, or other modifications.	Blocked
Web Communication / Message Boards	Sites that allow or offer Web based communication using any of the following mediums: E-mail (Web based), Chat, Instant Messaging, Message Boards, etc.	Allowed
Web Hosting / Personal Web Pages	Sites of organizations that provide top-level domain pages of Web communities or hosting services. Sites that host Web Chat services, on-IRC chat rooms, Chat sites via HTTP, home pages devoted to IRC, as well as sites that offer forums or discussion groups. Sites that promote or provide the means to practice illegal or unauthorized acts using computer-programming skills (hacking). Also sites containing ALL types of content such as GEO Cities.	Allowed

Table 8-1: Parental Control categories

If you are using ZoneAlarm Security Suite and you choose to block new categories, you may want to clean your browser cache to remove pages from newly blocked sites that may be stored there. Otherwise, anyone using your computer will have access to blocked content that has been stored in your browser's cache.

Chapter 9

E-mail protection

Worms, viruses, and other threats often use e-mail to spread from computer to computer. MailSafe protects your friends, co-workers, and others in your address book and helps keep destructive viruses from spreading. The Junk E-mail filter blocks out spam.

Topics:

- "Understanding e-mail protection," on page 147
- "Enabling Outbound MailSafe protection," on page 148
- "Customizing Outbound MailSafe protection," on page 148
- "Filtering junk e-mail (spam)," on page 150

Understanding e-mail protection

Attaching files to e-mail messages is a convenient way of exchanging information. However, it also provides hackers with an easy way of spreading viruses, worms, Trojan horse programs, and other malware.

The outbound MailSafe feature stops worms from mass-mailing themselves to everyone you know.

- Outbound MailSafe protection
- Enabling Outbound MailSafe protection
- Customizing Outbound MailSafe protection

Outbound MailSafe protection

Outbound MailSafe protection alerts you if your e-mail program tries to send an unusually large number of messages, or tries to send a message to an unusually large number of recipients. This prevents your computer from being used without your knowledge to send infected attachments to other people. In addition, Outbound MailSafe protection verifies that the program attempting to send the e-mail has permission to send e-mail messages.

Outbound MailSafe protection works with any e-mail application that uses SMTP.

Enabling Outbound MailSafe protection

For your security, Outbound MailSafe Protection is enabled by default. When Outbound protection is enabled, Outbound MailSafe settings apply to all programs with send mail privileges.

To enable or disable Outbound MailSafe Protection

1. Select **E-mail Protection**.
2. In the Outbound MailSafe Protection area, select **On** or **Off**.

Customizing Outbound MailSafe protection

By default, an Outbound MailSafe protection alert is displayed when your e-mail application attempts to send more than five e-mail messages within two seconds, or if an e-mail message has more than fifty recipients. You can customize these settings to extend the time interval, increase the number of messages and recipients allowed, or specify the e-mail addresses that are allowed to send e-mail from your computer.

- Enabling Outbound MailSafe protection by program
- Setting Outbound MailSafe protection options

Enabling Outbound MailSafe protection by program

When Outbound MailSafe protection is set to On, protection is enabled for all programs that have been granted permission to send e-mail.

You can customize Outbound MailSafe protection by enabling or disabling it for particular programs.

For information on setting permissions for a program, see "Setting permissions for specific programs," on page 101.

To enable or disable Outbound MailSafe protection for a program:

1. Select **Program Control**|**Programs**.
2. In the Programs column, right-click a program name, then select **Options**.
3. Select the **Security** panel.
4. In the Outbound MailSafe Protection area, select the check box labeled **Enable Outbound MailSafe Protection for this program**.

   To disable Outbound MailSafe protection, clear this check box.
5. Click **OK**.

Setting Outbound MailSafe protection options

By default, Outbound MailSafe Protection is activated when your computer attempts to send more than five e-mail messages within two seconds, or an e-mail message with more than 50 recipients.

Because even legitimate e-mail messages may have one or both of these characteristics, you may want to customize Outbound MailSafe protection settings to better meet your individual needs.

To customize Outbound MailSafe protection settings:

1. Select **E-mail Protection**, then click **Advanced**.

   The Advanced E-mail Protection dialog appears.
2. In the Display Outbound MailSafe Protection Alerts When area, choose your settings.

Too many e-mails are sent at once	An Outbound MailSafe protection alert appears when your computer attempts to send more than the specified number of e-mails within the specified time interval.
A message has too many recipients	An Outbound MailSafe protection alert appears when your computer attempts to send an e-mail message with more than the specified number of recipients.
If the sender's address is not in this list	An Outbound MailSafe protection alert appears when your computer attempts to send an e-mail whose originating address (i.e., the address in the **From:** field) does not appear on the list. To prevent ZoneAlarm security software from blocking all outgoing e-mail, make sure that your valid e-mail address appears on this list.

3. Click **OK**.

Filtering junk e-mail (spam)

Use the junk e-mail filter to prevent unsolicited junk e-mail (commonly referred to as *spam*) from cluttering your Inbox. The Junk E-mail filter supports Microsoft Outlook and Outlook Express (both referred to in this document simply as "Outlook").

During installation, ZoneAlarm security software adds the junk e-mail filter toolbar to your Outlook e-mail program's toolbar.

Figure 9-1: The junk e-mail filter toolbar

If you have installed ZoneAlarm security software but the junk e-mail filter toolbar does not appear in your Outlook toolbar, right-click in your Outlook toolbar and choose **ZoneAlarmOutlookAddin**.

The junk e-mail filter also adds three special folders to your Outlook folder list: ZoneAlarm Challenged Mail, ZoneAlarm Junk Mail, and ZoneAlarm Phishing Mail. When ZoneAlarm security software identifies an e-mail message as junk, phishing, or challenged, it puts the message in one of these folders. If you are using Outlook to access Hotmail, you must use the junk e-mail filter's spam blocking features and special folders instead of Hotmail's.

- Allowing or blocking e-mail from specific senders, companies, or lists
- Allowing or blocking e-mail from specific companies
- Adding contacts to the Allowed List
- Allowing e-mail from distribution lists
- Scanning your Inbox
- Reporting junk e-mail
- Reporting phishing e-mail
- Specifying junk e-mail message options
- Challenging e-mail from unknown senders
- Specifying your outbound e-mail server
- Customizing junk e-mail filter settings
- Viewing junk e-mail filter reports

Allowing or blocking e-mail from specific senders

Each time you send an e-mail to a new person, the junk e-mail filter automatically adds to the Allowed list, the address in the To field. Messages sent to you from those addresses will be put in your Inbox.

When you receive an e-mail from a sender on the Blocked list, the junk e-mail filter automatically moves the message to the Outlook folder named *ZoneAlarm Junk Mail.*

If an unwanted e-mail arrives in your Outlook Inbox, you can easily add the sender of that message to your Blocked People list.

To add e-mail addresses to your Allowed or Blocked list:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Allow Sender** or **Block Sender**.

Allowing or blocking e-mail from specific companies

The junk e-mail filter allows you to add all e-mail addresses originating from a particular company or network domain to your Companies Allowed or Blocked lists.

To add companies to your Allowed or Blocked list:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Allow Sender's Company** or **Block Sender's Company**.

   The junk e-mail filter adds the domain portion of the sender's address (for example, *example.com*) to the list of allowed or blocked addresses.

Adding contacts to the Allowed List

You can scan the default contacts folder in your e-mail program to add contacts to the list of senders from whom you wish to receive e-mail.

To add contacts to the Allowed List:

1. Open your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Populate Allowed List**.

Scanning your Inbox

You can scan the contents of your Inbox for phishing e-mail and spam. You can use the Scan Inbox option to scan IMAP, POP3, and Hotmail accounts created in Outlook Express, and IMAP, POP3 and Exchange server accounts in Outlook.

To scan your Inbox:

1. Open your Outlook or Outlook Express e-mail program.

2. Select the Inbox you want to scan.
3. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Scan selected Inbox**.

Allowing e-mail from distribution lists

If you receive or send e-mail to multiple addressees contained in a distribution list, the junk e-mail filter may block that list name unless it has been added to the Lists panel.

To allow e-mail from mailing lists:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Lists**.
3. Click **Add**.
4. Type the e-mail address of the distribution list into the text entry area, then click **OK**.

   The junk e-mail filter adds the distribution list's e-mail address to the list of allowed addresses.
5. Click **Close** to save your changes and close the Lists panel.

Reporting junk e-mail

The junk e-mail filter allows you to contribute instances of junk e-mail to the ZoneAlarm Collaborative Filter database.

The junk e-mail filter never sends e-mail of any type from your computer without your permission. When you contribute junk e-mail to the Collaborative Filter database, you can choose to send either the actual e-mail or a digitally processed (sometimes referred to as "hashed") summary of the e-mail that removes all content, headers, and personally identifiable information from the message. Sending the entire message enables complete analysis of the contents; sending a digitally processed summary of the message ensures complete privacy.

MailFrontier, a trusted ZoneAlarm partner, manages the Collaborative Filter database for ZoneAlarm. You can view the full text of MailFrontier's privacy policy at: http://www.mailfrontier.com/privacy.html

To report junk e-mail:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.
2. In the junk e-mail filter toolbar:
   - To send the junk e-mail itself, click **ZoneAlarm Options**, then choose **Report Junk E-mail**.
   - To send a digitally processed summary of the junk e-mail, click **Junk**.

3. In the **Contribute E-mail** dialog box, click **OK**.

   The junk e-mail filter reports the junk e-mail to the Collaborative Filter database and moves the message to the special Outlook folder **ZoneAlarm Junk Mail**.

To restore e-mail that was incorrectly identified as junk, select the e-mail in the ZoneAlarm Junk Mail folder, and click Unjunk. The e-mail will be restored to your Outlook Inbox.

Reporting phishing e-mail

The junk e-mail filter allows you to report instances of phishing e-mail referred to as *phishing*) to ZoneAlarm. When phishing mail is detected for the first time, a popup appears, asking if you would like to send the phishing mail to ZoneAlarm for analysis. If you choose Yes, all future phishing messages will be sent without prompting you for confirmation. If you choose No, your choice will be reflected in the Configure Preferences dialog box.

The junk e-mail filter never sends e-mail of any type from your computer without your permission. When you report phishing e-mail, the junk e-mail filter forwards the complete and original message to ZoneAlarm.

ZoneAlarm never divulges your e-mail address, name or other personal information contained in a phishing e-mail except as required to investigate and prosecute the originator of the phishing message.

ZoneAlarm forwards selected portions of the reported message to government and law enforcement agencies with jurisdiction over e-mail fraud. These agencies are required by law to protect the confidentiality of the information contained in the message. ZoneAlarm separately informs individuals or institutions threatened by forwarding to them only the information required to alert them.

To report phishing e-mail:

1. In your Outlook or Outlook Express e-mail program, select an e-mail.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options**, then choose **Report Phishing E-mail**.
3. In the **Contribute E-mail** dialog box, click **OK**.

   The junk e-mail filter reports the phishing e-mail to ZoneAlarm and moves the message to the special Outlook folder *ZoneAlarm Phishing Mail*. If you are using

Outlook to access Hotmail, you must use the junk e-mail filter's spam blocking features and special folders instead of Hotmail's.

MailFrontier, a trusted ZoneAlarm partner, manages the processing of phishing e-mail for ZoneAlarm. You can view the full text of MailFrontier's privacy policy at: http://www.mailfrontier.com/privacy.html

Specifying junk e-mail message options

The junk e-mail filter uses three message filtering techniques: *collaborative filter*, *message filters*, and *foreign language filters*. Filter settings determine how messages are treated when received from unknown senders.

Collaborative Filter

Collaborative filtering uses information extracted from junk e-mail reported by you and other ZoneAlarm security software users to determine whether new messages received from unknown users is spam.

Message Filters

Message filters use heuristic rules to analyze e-mail for characteristics common to various types of junk e-mail.

Foreign language filters

Foreign language filters block e-mail containing non-european languages. (The junk e-mail filter automatically manages e-mail in common european languages such as French, German, or Spanish.)

To customize message filtering options:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options | Configure Preferences | Messages**.

Collaborative Filter	In the area, move the slider to adjust the responsiveness to the characteristics of junk e-mail reported by other ZoneAlarm security software users.
Message Filters	Move the slider to adjust the responsiveness to common junk e-mail. You can also adjust the responsiveness to specific categories of junk e-mail.
Language Filters	In the area, click Configure then choose which languages to block.

3. Click **Close**.

Challenging e-mail from unknown senders

You can choose to have the junk e-mail filter reply to an e-mail from an unknown sender with a challenge e-mail. Because junk e-mail seldom contains a valid return address, an unanswered challenge confirms that the e-mail is probably junk.

The challenge e-mail instructs the recipient to click a button in the message to validate that he or she was the author of the message. Clicking the button directs the junk e-mail filter to move the e-mail from the special Outlook folder **ZoneAlarm Challenged Mail** folder to your Outlook Inbox.

For messages from an unknown sender, you can choose whether to always send a challenge e-mail, to send a challenge only when the incoming message appears to be junk e-mail, or to never send a challenge. In addition you can customize the challenge e-mail that is sent to users.

To enable challenge e-mails:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Challenges**.
3. In the Challenges area, use the slider to choose when to send a challenge e-mail.

High	ZoneAlarm security software will challenge all e-mails that you receive unless they are known as good to either you (on your allowed lists) or to MailFrontier (known good senders). Any e-mail message that is received and can be classified immediately as junk gets sent directly to the ZoneAlarm Mail folder for later deletion and does NOT get a challenge issued.
Low	ZoneAlarm security software will challenge uncertain e-mail. ZoneAlarm security software will only challenge e-mails that it cannot determine with certainty are spam or are good. This is typically a small percentage of the e-mail you receive.
Off	Challenge e-mails will not be sent. ZoneAlarm security software will not send challenge e-mails. Move the slider up to turn on e-mail challenges to eliminate junk e-mail sent by spammer computers.

4. To add a personal message to the standard challenge e-mail, click **Personalize**, type your name and your personal message, then click **OK**.

5. Click **Close**.

   The junk e-mail filter moves the message to the **ZoneAlarm Challenged Mail**. folder

While waiting for the response to a challenge message, the junk e-mail filter stores your e-mail address. As soon as the challenge has been completely processed, the junk e-mail filter discards the address. If you experience problems sending challenge e-mails, see "Specifying your outbound e-mail server," on page 156.

Specifying your outbound e-mail server

To send challenge e-mails, the junk e-mail filter requires the ability to send e-mail. In most cases the junk e-mail filter uses Outlook's default outbound mail server. If you experience problems sending challenge e-mails, you may need to specify the name of your outbound e-mail server.

To specify the name of an outbound e-mail server:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Challenges**.
3. In the Challenge Content area, click **E-mail Server**.
4. Type the name of your outbound e-mail server, then click **OK**.
5. Click **Close**.

Customizing junk e-mail filter settings

By default, the junk e-mail filter retains phishing e-mail messages in the **ZoneAlarm phishing Mail** folder until you manually delete them. You can specify how long e-mail messages are stored in the **ZoneAlarm Junk Mail** and **ZoneAlarm Challenged Mail** folders, as well as automate fraud e-mail reporting, and configure wireless device forwarding. In addition, if you could like to scan more than one Outlook Inbox, you can specify those settings here.

To specify storage duration for junk e-mail:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Settings**.
3. In the Junk Folder Settings area, click **Configure**.

4. Type the number of days to retain suspected junk e-mail in the **ZoneAlarm Junk Mail** and **ZoneAlarm Challenged Mail** folders.

   The junk e-mail filter moves e-mail that has been in the folder for the specified number of days without being validated into Outlook's Deleted Items folder.

5. Click **Close**.

To configure a wireless device:

1. Start your Outlook or Outlook Express e-mail program
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Settings**.
3. In the Wireless Device Support area, click **Configure**.
4. In the **ZoneAlarm Wireless Support** dialog box, type the e-mail address of your wireless device.

   You can also choose to forward only e-mail headers, and to specify the number of validate messages forwarded to your wireless device in a 24-hour period.

5. If you need to specify a non-default e-mail server, click **E-mail Server**, type the name of your outbound e-mail server, then click **OK**.

   Click **Close** to save your changes.

To enable automatic reporting of phishing e-mail:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Settings**.
3. In the Auto Report Fraud E-mail area, select the **Enable auto reporting...** check box.
4. Click **Close.**

To customize confirmation messages:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Settings**.
3. In the Show Confirmations area, specify the settings you want.

Contribute Junk Email	Displays an alert prior to sending junk e-mail to ZoneAlarm.
Contribute Phishing Email	Displays an alert prior to sending phishing e-mail to ZoneAlarm.

4. Click **Close**.

To configure multiple Outlook inboxes:

1. Start your Outlook or Outlook Express e-mail program.
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Settings**.
3. In the Outlook Multiple Inbox Support area, select the check box **Support scanning of multiple Inbox in Microsoft Outlook**.

This feature is supported for Outlook 2000, 2002 (XP), and 2003 only and is enabled by default.

Restoring e-mail incorrectly identified as junk

The junk e-mail filter adds three special folders to your Outlook folder list: **ZoneAlarm Challenged Mail**, **ZoneAlarm Junk Mail**, and **ZoneAlarm Phishing Mail**. When ZoneAlarm security software identifies an e-mail message as junk, fraudulent, or challenged, it puts the message in one of these special folders.

If you are using Outlook to access Hotmail, you must use the junk e-mail filter's spam blocking features and special folders instead of Hotmail's.

You can restore mail that the junk e-mail filter incorrectly placed in a special folder to your Outlook Inbox.

To restore e-mail incorrectly identified as junk:

1. In your Outlook or Outlook Express e-mail program, in the **ZoneAlarm Challenged Mail**, **ZoneAlarm Junk Mail**, or **ZoneAlarm Phishing Mail** folder, choose an e-mail.
2. In the junk e-mail filter toolbar, click **Unjunk**.

   The junk e-mail filter restores the selected message to your Outlook Inbox.

Viewing junk e-mail filter reports

Use the junk e-mail filter's Reports panel to view a summary of mail processing activity.

To view junk e-mail filter reports

1. Start your Outlook or Outlook Express e-mail program
2. In the junk e-mail filter toolbar, click **ZoneAlarm Options** | **Configure Preferences** | **Reports**.
3. Choose one of the four report types:

Junk by Day	The total number of legitimate and junk e-mails received by day.
Reasons	The reasons the junk e-mail filter blocked incoming e-mails by day

Total History Junk by Day	The total number of legitimate and junk e-mails received since ZoneAlarm security software was installed.
Total Reasons	The total number of reasons the junk e-mail filter blocked incoming e-mails since ZoneAlarm security software was installed.

4. Click **Close** to close the Reports panel.

Chapter 10

Identity protection

With the rise of e-commerce, electronic record keeping, and mass financial mailings, the incidence of identity theft has increased in recent years. Hackers can use malware to intercept your personal information online, while thieves can steal CDs and laptops containing customer information, or they can intercept sensitive mail items (such as pre-approved credit card offers) that include personal data.

ZoneAlarm security software helps protect your personal data online and out in the everyday world. ID Lock keeps your personal information safe from hackers and identity thieves. The ZoneAlarm Identity Protection Center offers resources that help you prevent, detect, and, if necessary, recover from identity theft.

Topics:

- "Understanding the ID Lock feature," on page 160
- "About myVAULT," on page 163
- "Using the Trusted Sites list," on page 166
- "Identity Protection Center," on page 168

Understanding the ID Lock feature

Every time you or someone else using your computer enters personal information into an e-mail message or Web form—such as your credit card number, address, or social security

number— it is possible that the information could be stolen. To help prevent that from happening, the ID Lock ensures that your personal information is only sent to sites you trust.

The ID Lock feature provides a secure area called myVAULT, where you can store personal information that you want to protect. The contents of myVAULT are blocked from being transmitted to unauthorized destinations, whether by you, someone else using your computer, or by a Trojan horse attempting to transmit your personal information.

- How your personal information is protected
- Setting the ID Lock protection level

How your personal information is protected

ZoneAlarm security software prevents your personal information from being transmitted without your authorization, whether in e-mail or on the Web.

E-mail transmission

When you or someone using your computer attempts to send myVAULT data in an e-mail message, ZoneAlarm security software displays an alert asking you whether to allow the information to be sent. If you want to always allow or always block the information from being sent to this destination, before clicking Yes or No select the check box labeled **"Do you want to remember this answer..."** to add the destination to your Trusted Sites list with the corresponding permission set automatically. For example, if you were to select the "Do you want to remember this answer..." check box and then click **Yes**, the destination would be added to the Trusted Sites list with the permission set to **Allow**. Conversely, if you were to click **No**, the permission would be set to **Block**.

When responding to an ID Lock alert that is the result of an e-mail transmission, clicking the **"Do you want to remember this answer..."** check box adds the domain of the intended recipient's e-mail server—not the e-mail recipient—to the Trusted Sites list. For example, if you were to allow myVAULT data to be transmitted to your contact john@example.com, and you chose to remember that answer, the next time myVAULT data is sent to ANY contact on example.com's e-mail server, the transmission would be allowed and you would not see an alert.

Web transmission

When transmitting myVAULT data on the Web, ZoneAlarm security software allows or blocks the transmission according to the permission for the domain in the Trusted Sites list. As with e-mail transmission of myVAULT contents, if you choose to remember your response to an ID Lock alert for a particular Web site, that Web site will be added to the Trusted Sites list automatically with the permission set accordingly.

IM transmission

When transmitting myVAULT data in an Instant Messaging conversation, ZoneAlarm security software prevents the information from being received.

Figure 10-1 shows an instant messaging conversation in which information that is stored in myVAULT is transmitted. The description of the item stored in myVAULT (in this example, My Visa Card) appears in brackets.

Figure 10-1: Transmission of myVAULT contents

Figure 10-2 shows how the transmitted information is displayed to the recipient. The protected information is replaced with asterisks so that it is unreadable.

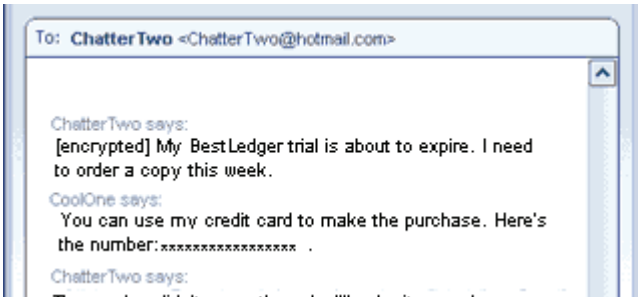


Figure 10-2: Receipt of myVAULT contents

Setting the ID Lock protection level

The ID Lock is disabled by default. By enabling the ID Lock, you ensure that the data entered in myVAULT will be protected.

ZoneAlarm security software keeps track of the number of items stored in myVAULT and displays the number of times your information was protected.

To set the ID Lock protection level:

1. Select **Identity Protection**.

2. In the Identity Lock area, specify the desired protection level.

High	Prevents the contents of myVAULT from being sent to unauthorized destinations. ZoneAlarm security software will block transmission of your data silently. If you are using a shared computer, this setting is recommended for maximum security.
Medium	Alerts you when your identity information is about to be sent to destinations not listed on the Trusted Sites list. This is the default setting.
Off	Identity protection is disabled. The contents of myVAULT can be sent to any destination, whether or not it appears on the Trusted Sites list.

About myVAULT

The myVAULT feature provides a secure area for entering your critical personal data—data that you want to protect from hackers and identity thieves. When it detects an attempt to send data stored in myVAULT to a destination, ZoneAlarm security software determines whether the information should be blocked or allowed. By default, ZoneAlarm security software encrypts myVAULT data as it is entered, storing only the hash value of the data rather than the data itself. Encrypting the data keeps your information secure, as data cannot be retrieved using the hash value.

- Adding data to myVAULT
- Editing and removing myVAULT contents

Adding data to myVAULT

While you can store any type of information in myVAULT, it is a good idea only to store information that you wish to keep secure, such as credit card numbers and identification information. If you were to store information such as your country of residence (for example, Canada) in myVAULT separately from the rest of your address, any time you typed "Canada" into an online Web form, ZoneAlarm security software would block transmission of the data.

If you're unsure of the type of information that should be entered into myVAULT, refer to the pre-defined categories for guidance. To access the list of categories, select **Identity Protection** | **myVAULT**, then click **Add**.

To add information to myVAULT:

1. Select **Identity Protection|myVAULT**.

2. Click **Add**.

   The Add information to myVAULT dialog box will appear.

   For maximum protection, ZoneAlarm security software encrypts myVAULT data by default. If you do not want to encrypt the data as you enter it, clear the **Use one-way encryption**... check box.

3. Type a description of the item you are adding.

ZoneAlarm security software displays the item description in ID Lock alerts. Be sure that the description you enter is different from the value of the item to be protected. If the information to be protected and the description contain some or all of the data, you may receive multiple ID Lock alerts.

4. Select a category from the drop-down list.

Access PIN	Personal access code or other ID number. Maximum of 6 characters. For added security, Access PINs are always encrypted.
Address	Maximum 30 characters.
American Express card	For added security, ZoneAlarm security software does not record the last 5 digits of your American Express card number.
Bank account	Maximum 14 characters.
Credit card	For added security, ZoneAlarm security software does not record the last 4 digits of your credit card number.
Driver's license	Maximum 15 characters.
eBay password	The password you use to access the eBay Web site. Your eBay password can only be sent to eBay. Maximum 20 characters.
E-mail Address	Maximum 60 characters.
International tax ID	Maximum 15 characters.
Mother's maiden name	Maximum 30 characters.
Name	Maximum 30 characters.
Passport number	US passport number or other International ID number. Maximum 30 characters.
Password	Enter the password to be protected. Maximum 20 characters.
Phone	Separators such as parentheses and dashes are not allowed. Maximum 13 characters.
US Social Security number	Requires 9 digits.

Other	Use this field to enter items that either do not correspond to any of the pre-configured categories, or which exceed the character limit for the corresponding category. Maximum 30 characters.

5. Type the data to be protected.

Data encryption is enabled by default. If you do not want to encrypt your data, clear the **Use one-way encryption...** check box. Because of the sensitive nature of the data, PIN numbers, passwords, the last four digits of your social security number, and the last four digits of your credit card numbers will always be displayed as asterisks, whether or not you choose to encrypt them.

To disable the encryption confirmation that appears by default, select **Identity Protection** | **myVAULT**, then click **Options**. Clear the **Show encryption confirmation** check box.

Asterisks will appear in place of the data you entered and an encrypted form of your data will be stored in myVAULT. ZoneAlarm security software will compare the encrypted data with your outgoing messages.

6. Specify whether you want the information to be protected when using Web, E-mail, and Instant Messengers (if available in your version of the product).

7. Click **OK** to save your changes.

Editing and removing myVAULT contents

In the myVAULT panel you can modify the encryption setting, remove myVAULT contents, and edit unencrypted data. Because encrypted data is displayed in asterisks, it is unreadable and therefore cannot be edited.

To edit myVAULT contents:

1. Select **Identity Protection**|**myVAULT**.

2. Select the item you want to edit, then click **Edit**.

   The Edit information from myVAULT dialog appears.

3. Modify data as necessary, then click **OK** to save your changes.

To remove myVAULT contents:

Select the item you want to remove, then click **Remove**.

If you remove the last item in myVAULT, the ID Lock protection level will be set to Off. If you later add items to myVAULT, the protection level will be reset to the default Medium setting.

Using the Trusted Sites list

The myVAULT feature provides a secure area for entering your critical personal data—data that could be used by hackers and identity thieves. When it detects an attempt to send data stored in myVAULT to a destination, ZoneAlarm security software determines whether the information should be blocked or allowed, by making sure the destination is one you trust.

There are two kinds of sites that can appear on the Trusted Sites list: Security Alliance and Custom. Security Alliance sites are sites that ZoneAlarm, a Check Point Software Technologies, Inc. Company has authenticated to ensure they are not fraudulent. Custom sites are sites you add to the list.

- Viewing the Trusted Sites list
- Adding to the Trusted Sites list
- Editing and removing trusted sites

Viewing the Trusted Sites list

In addition to listing sites you trust with your personal information, you can add sites to the list that you explicitly do *not* want to trust, such as known spam or chat sites, and prevent information from being sent to them.

To see the Trust Sites list, select **Identity Protection**|**Trusted Sites**. The Add Trusted Site dialog appears.

The Trusted Sites list also lets you specify which sites are allowed to send your password as *clear text*. Because clear-text passwords are unencrypted, they can easily be viewed by others if intercepted during transmission.

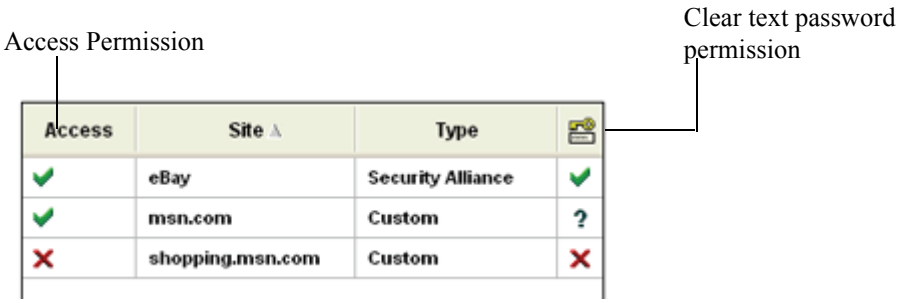


Figure 10-3: Trusted Sites list

Access permission

Specifies whether ZoneAlarm security software will allow, block, or alert you before sending myVAULT contents to the listed destinations. To modify the permission for a site, click beside the site in the Access column and choose **Allow, Block**, or **Ask**.

Site

Displays the domain of the site.

Type

Specifies whether the site is a Security Alliance partner or a Custom site.

Clear Text password

Specifies whether ZoneAlarm security software will allow, block, or alert you before sending your password as clear text to the listed destinations. To modify the permission for a site, click beside the site in the Clear Text password column and choose **Allow, Block**, or **Ask**.

Site Entry Details

In addition to the site name and type, the Entry Details box displays the site IP Address and the date and time you last accessed the site.

Adding to the Trusted Sites list

There are two types of sites that appear on the Trusted Sites list: Custom and Security Alliance. Custom sites are sites that you add to the list. Security Alliance partner sites are sites that ZoneAlarm has verified are legitimate and has added automatically.

Custom sites are trusted at the domain level, therefore each sub-domain you want to trust must be added separately. For example, www.msn.com and shopping.msn.com would need to be added separately. Security Alliance sites explicitly trust all sub-domains, so you do not need to create an entry for each sub-domain you want to trust.

To add a site to the Trusted Sites list:

1. Select **Identity Protection**|**Trusted Sites**, then click **Add**.

   The Add Trusted Site dialog appears.

2. Type the URL of the site (omit http://www), then click **OK**.

   After you click OK, ZoneAlarm security software verifies the site address and records the IP address. This process can take several seconds.

3. Modify the site permissions as desired.

   By default, access and clear text password permissions for Custom sites are set to Ask.

Editing and removing trusted sites

In the Trusted Sites panel, you can modify the access permission for a site, and edit or remove Custom sites. Although you can modify the permissions for Security Alliance partner sites, you cannot edit or remove the site entry.

To edit a Custom site:

1. Double-click the site you want to edit.

   The Edit trusted site dialog appears.

2. Edit the site as necessary, then click **OK** to save your changes.

To remove a custom site:

Right-click the site you want to remove, then click **Remove**.

Identity Protection Center

The ZoneAlarm Identity Protection Center is a Web site that helps you prevent, detect, and, if necessary, recover from identity theft. (Identity theft is a crime in which someone exploits your personal information for their own gain.) The Identity Protection Center

includes identity protection tips as well as resources for monitoring the use of your personal information and for recovering from identity theft.

To visit the Identity Protection Center:

1. Go to **Identity Protection**.
2. In the Identity Protection Center area, click **Go to ZoneAlarm Identity Protection Center**.

Chapter 11

Hard Drive Encryption for Laptops

Encrypting your hard drive is important because if your computer is lost or stolen, a hacker can remove your drive and read it without even knowing your Windows logon name and password. But, if your drive is encrypted, your sensitive data is protected—thieves are locked out of it.

Topics:

- "Do I need Hard Drive Encryption for Laptops?," on page 172
- "Using Hard Drive Encryption for Laptops," on page 173
- "Installing Hard Drive Encryption for Laptops," on page 174
- "Hard Drive Encryption Main panel," on page 175
- "Hard Drive Encryption Advanced panel," on page 176
- "Troubleshooting Hard Drive Encryption," on page 177

Do I need Hard Drive Encryption for Laptops?

Not everyone needs to encrypt their hard drive, but full hard drive encryption is ideal for:

- anyone who has identity information, such as tax forms or financial account data, on their laptop and thinks there is a risk of their laptop being lost or stolen (e.g., while traveling or in public places)

- small business owners and others who have proprietary or private data, such as client files, on their laptop

What is Hard Drive Encryption?
Hard Drive Encryption makes everything on your computer unreadable to unauthorized users. Your own encryption password is required before your computer fully boots up. Your full hard disk is encrypted, including deleted and temporary files, which protects your sensitive data if your disk is stolen or lost. This prevents hackers from breaking into your operating system by removing your disk and using bypass tools or alternative boot media.

Using Hard Drive Encryption for Laptops

Hard Drive Encryption is not available until you install it from **Additional Services** in the ZoneAlarm window. (Some versions of the product do not include the option to install this feature.)

How does it affect my day-to-day computer usage?

- **Another login at startup:** Before your Windows login screen appears, you log in to a Hard Drive Encryption screen when you start your computer. This gives you secure access to your encrypted operating system.
- **The rest is silent and invisible:** Your files and desktop are silently decrypted when you access them and encrypted when you close them, but this process is invisible to you.

When your disk is encrypted, your computer will be able to go into sleep mode, but not hibernation mode.

Topics:

- "Do I need Hard Drive Encryption for Laptops?," on page 172
- "Installing Hard Drive Encryption for Laptops," on page 174
- "Creating your recovery disk," on page 175
- "Hard Drive Encryption Main panel," on page 175
- "Hard Drive Encryption Advanced panel," on page 176
- "Troubleshooting Hard Drive Encryption," on page 177

Installing Hard Drive Encryption for Laptops

If you have a license that supports Hard Drive Encryption, you can install it from the ZoneAlarm window.

To install or reinstall Hard Drive Encryption for Laptops:

1. Back up copies of your valued files.
2. Have a CD, floppy disk, or blank USB stick on hand for recovery disk creation.

If you create your recovery disk with a CD, you will need CD-burning software that supports burning an ISO image. Some CD-burning applications do not have ISO-burning capability. To find one that does, try searching trusted online software download sources (for example, http://download.cnet.com/) with the search text "free software to burn ISO."

3. Select **Hard Drive Encryption** under the **Additional Services** side panel.

   The installation and recovery disk wizards will appear in sequence and step you through:

   - Creating an account for support, and then one for logging in to Hard Drive Encryption.
   - Installation and restart.
   - Creating your recovery disk. See "Creating your recovery disk," on page 175.

   After installation and recovery disk creation, there is nothing you need to configure. Hard Drive Encryption automatically encrypts all internal hard drives, but does not encrypt any external hard drives.

During encryption:

Encryption starts automatically and runs in the background. It may take a few hours for full encryption to complete. You can use your laptop and turn it on and off during this process, though decryption pauses while your computer is off.

Hard Drive Encryption Main panel

Main panel options:

Run the Recovery Disk Wizard	Steps you through creating a recovery disk. If you change your password you need to then create a new recovery disk because your new authentication must be incorporated into your recovery media. See "Creating your recovery disk," on page 175.
Encryption Status bar	Shows the progress and completion of encryption after you install Hard Drive Encryption for Laptops. See "The Encryption Status bar," on page 176.

Creating your recovery disk

Hard Drive Encryption for Laptops does not start encrypting until you create a recovery disk with the Recovery Wizard.

Why do you need to use the Recovery Disk Wizard?

- **To create a way to decrypt in case of system failure:** You need to create a recovery disk because it's the only way you will be able to access everything on your disk if you experience a system failure that blocks you from accessing the Hard Drive Encryption login screen. The recovery disk lets you decrypt your "locked" disk so you can retrieve your data.
- **In case you ever forget your Hard Drive Encryption password:** You need to upload data to the support team, as this is the only way you will be able to reset your Hard Drive Encryption password if you forget it. You can only upload this data with the Recovery Wizard.

To create a recovery disk:

1. Have a blank CD, floppy disk, or USB memory stick ready, and make sure that your computer supports copying or burning to it.
2. If the Recovery Wizard is not already open:

   Click **Hard Drive Encryption** in the navigation bar, and then click **Run the Recovery Wizard**.
3. In the Recovery Wizard, follow the instructions and prompts that appear.

   On the final **Create Recovery Disk** step, what you do depends on what media you are using:

Floppy or USB	Choose the inserted floppy disk or USB stick from the drop-down menu. The Recovery Wizard copies a disk image to the floppy or USB stick.

CD ISO images	When you are finished with the Recovery Wizard, select the ISO image you saved and burn it to CD with your CD burning software. If your CD-burning program does not have ISO-burning capability, you can find one that does. Try searching trusted online software download sources (for example, http://download.cnet.com/) with the search text "free software to burn ISO."

4. Put your recovery disk in a safe, secure place.

   If you ever need to use your recovery disk to decrypt and recover data, insert the disk, restart your computer, and then follow the instructions that appear.

It's a good idea to print out "How to decrypt in case of system failure," on page 178 and keep it with your recovery disk.

The Encryption Status bar

The Encryption Status bar on the **Hard Drive Encryption** | **Advanced** panel in ZoneAlarm shows the progress and completion of encryption after you install Hard Drive Encryption.

Encryption takes place in the background and does not affect your system experience. While individual files and your desktop are invisibly decrypted on access and encrypted when you close them, the Encryption Status bar maintains a 100% status to indicate you have full encryption protection.

Hard Drive Encryption Advanced panel

Advanced panel options:

Remove Hard Drive Encryption	Removes Hard Drive Encryption and decrypts your system. You can reinstall at any time. See "Stopping or removing Hard Drive Encryption," on page 177

Stopping or removing Hard Drive Encryption

If Hard Drive Encryption is installed, it's active on your system. There is no on or off button for it, but you can remove it and reinstall it at any time.

Even if you uninstall ZoneAlarm, Hard Drive Encryption remains installed so that your system is still encrypted.

To uninstall Hard Drive Encryption, use the Remove function on the Hard Drive Encryption panel.

To remove Hard Drive Encryption:

1. Open ZoneAlarm by right-clicking the ZoneAlarm icon in the system tray.
2. Go to the **Hard Drive Encryption** | **Advanced** panel.
3. Click the **Remove Hard Drive Encryption** button.

   Decryption starts, and progress is shown on the Hard Drive Encryption panel.

   Decryption may take a few hours, and after that Hard Drive Encryption will be completely uninstalled. You can use your computer and turn it on and off during this process, though decryption pauses when your computer is off.

You can reinstall at anytime by clicking Hard Drive Encryption under Additional Services.

Troubleshooting Hard Drive Encryption

Topics:

- "What to do if you forget your password or username:," on page 178
- "How to decrypt in case of system failure," on page 178
- "Stopping or removing Hard Drive Encryption," on page 177

Tip: Check the ZoneAlarm Readme for Known Issues and workarounds: From the Windows Start menu, choose All Programs | ZoneAlarm | Readme. See the Hard Drive Encryption section.

What to do if you forget your password or username:

If you forget your Hard Drive Encryption login credentials:

- Click the **Help** button on the Hard Drive Encryption login screen. Use the contact information that appears. We will authenticate your identity with the security questions you created during installation, and help you regain access to your computer.

Tips:

If you forget your username	By default, your username is the same as your Windows logon username.
If you haven't completed the upload step in the Recovery Disk Wizard	Get help through support live chat at http://www.zonealarm.com/chat.

How to decrypt in case of system failure

If your hard drive crashes and you need to recover the data on your disk but can't access the login screen, you can decrypt your data with the recovery disk you prepared with the Recovery Wizard.

If a system crash locks you out of access to your login screen, you need to use your recovery disk to decrypt your drive in order to recover your files.

Tip: Print these steps and keep them with your recovery disk.

To decrypt when you need to recover your data:

1. Locate the recovery disk you created.

If you lost your Hard Drive Encryption recovery disk, contact support at http://www.zonealarm.com/chat.

2. Insert your recovery disk and restart your computer.
3. Follow the instructions that appear.
   - Because it is a pre-boot environment, use the **Tab** key to move the cursor and press **Enter** to make a selection. (The mouse won't work.)
   - Once decryption starts, the percentage of the decryption is displayed. It can take up to a few hours to complete.
   - When decryption is complete, you'll be prompted to reboot.

4. Be sure to eject the recovery disk before you power back up.

After you power down, eject the recovery disk, otherwise you'll be booted into the recovery environment again.

5. To reactivate Hard Drive Encryption, you need to:
   - First, remove it. See "Stopping or removing Hard Drive Encryption," on page 177.
   - Then, reinstall it from under **Additional Services.**

Chapter 12

Managing Alerts and Logs

Whether you're the type of person who wants to know everything that happens on your computer—or you only want to know that your computer is secure, ZoneAlarm security software accommodates you. You can be notified by an alert each time ZoneAlarm security software acts to protect you, or only when an alert is likely to have resulted from hacker activity. You can also choose to log all alerts, only high-rated alerts, or alerts caused by specific traffic types.

Topics:

- "Understanding alerts and logs," on page 182
- "Setting basic alert and log options," on page 182
- "Controlling the number of alerts," on page 183
- "Setting event and program log options," on page 184
- "Using SmartDefense Advisor and Hacker ID," on page 191

For information about suppressing most alerts while playing games on your computer, see "Game Mode," on page 193.

Understanding alerts and logs

Understanding and reducing alerts

To learn about the various kinds of ZoneAlarm security software alerts you may see, see Chapter 4,"Understanding and reducing alerts," starting on page 59.

Understanding the alerts and logs panel

ZoneAlarm security software alert and logging features keep you aware of what's happening on your computer without being overly intrusive, and enable you to go back at any time to investigate past alerts.

Expert rule options let you track not only blocked Internet traffic, but allowed traffic as well, giving advanced users the option of maximum information for customizing security rules for their environment.

About event logging

By default, ZoneAlarm security software creates a log entry every time traffic is blocked, whether an alert is displayed or not. Log entries record the traffic source and destination, ports, protocols, and other details. The information is recorded to a text file named ZALOG.txt, stored in the Internet Logs folder. Every 60 days, the log file is archived to a dated file so that it doesn't become too large.

You can choose to prevent specific categories of events from being logged—for example, you may want to create log entries only for firewall alerts, or suppress entries for a particular type of Program alert. You can also have ZoneAlarm security software log specific types of traffic you have decided to allow, by creating expert rules with tracking features enabled.

Setting basic alert and log options

Basic alert and log options let you specify the type of event for which ZoneAlarm security software displays an alert and for which events it creates a log entry.

- Setting the alert event level
- Setting event and program logging options

Setting the alert event level

The Alert Events Shown control, in the main panel of Alerts & Logs, lets you control the display of alerts by rating. Program and ID Lock alerts are always displayed, because they ask you to decide whether to grant permission.

To set the alert event level:

1. Select **Alerts & Logs**.
2. In the Alert Events Shown area, select the desired setting.

High	Displays an alert for every security event that occurs, both high-rated and medium-rated.
Med	Displays only high-rated alerts, which are most likely a result of hacker activity.
Off	Displays Program and ID Lock alerts only. Informational alerts are not displayed.

Setting event and program logging options

Use the Event Logging and Program Logging areas to choose what types of informational alerts and program alerts will be logged.

To enable or disable event logging and program logging:

1. Select **Alerts & Logs**.
2. In the Event Logging area, select the desired setting.

On	Creates a log entry for all events.
Off	No events are logged.

3. In the Program Logging area, specify the log level.

High	Creates a log entry for all program alerts.
Med.	Creates a log entry for high-rated program alerts only.
Off	No program events are logged.

Controlling the number of alerts

You can specify whether you want to be alerted to all security and program events, or if you only want to be notified of events that are likely a result of hacker activity.

- If you want to suppress most alerts while playing a computer game, see "Game Mode," on page 193.

- For details about how to reduce certain types of alerts, and why each alert happens, see **"Understanding and reducing alerts," on page 59**.

Showing or hiding firewall and program alerts

The Alert Events panel gives you more detailed control of alert display by allowing you to specify the types of blocked traffic for which Firewall and Program alerts are displayed.

To show or hide firewall or program alerts:

1. Select **Alerts & Logs**, then click **Advanced**.

   The Alert & Log Settings dialog appears.

2. Select the **Alert Events** panel.
3. In the Alert column, select the type of blocked traffic for which ZoneAlarm security software should display an alert.
4. Click **Apply** to save your changes.

Setting event and program log options

You can specify whether ZoneAlarm security software keeps record of security and program events by enabling or disabling logging for each type of alert.

- Formatting log appearance
- Customizing event logging
- Customizing program logging
- Viewing log entries
- Viewing the text log
- Archiving log entries

Formatting log appearance

Use these controls to determine the field separator for your text log files.

To format log entries:

1. Select **Alerts & Logs**, then click **Advanced**.

   The Advanced Alerts and Log Settings dialog appears.

2. Select the **Log Control** panel.

3. In the Log Archive Appearance area, select the format to be used for logs.

Tab	Select Tab to separate fields with a tab character.
Comma	Select Comma to separate fields with a comma.
Semicolon	Select Semicolon to separate log fields with a semicolon.

Customizing event logging

By default, ZoneAlarm security software creates a log entry when a high-rated firewall event occurs. You can customize Firewall alert logging by suppressing or allowing log entries for specific security events, such as MailSafe quarantined attachments, Blocked non-IP packets, or Lock violations.

To create or suppress log entries based on event type:

1. Select **Alerts & Logs**.
2. Click **Advanced**.

   The Advanced Alerts and Logs dialog box appears.
3. Select **Alert Events**.
4. In the Log column, select the type of event for which ZoneAlarm security software should create a log entry.
5. Click **Apply** to save your changes.
6. Click **OK** to close the Alert & Log Settings dialog.

Customizing program logging

By default, ZoneAlarm security software creates a log entry when any type of Program alert occurs. You can customize Program alert logging by suppressing log entries for specific Program alert types, such as New Program alerts, Repeat Program alerts, or Server Program alerts.

To create or suppress log entries based on event type:

1. Select **Alerts & Logs**.
2. In the Program Logging area, click **Custom**.
3. In the Program Logs column, select the type of event for which ZoneAlarm security software should create a log entry.
4. Click **Apply** to save your changes.
5. Click **OK** to close the Alert & Log Settings dialog.

Viewing log entries

You can view log entries two ways: in a text file using a text editor, or in the Log Viewer. Although the format of each type of log differs slightly, the general information contained in the log is the same.

To view the current log in the Log Viewer:

1. Select **Alerts & Logs | Log Viewer**.
2. Select the number of alerts to display (from 1 to 999) in the alerts list.

   You can sort the list by any field by clicking the column header. The arrow (^) next to the header name indicates the sort order. Click the same header again to reverse the sort order.
3. Select the type of alert you want to view:

Anti-virus	Displays the Date/Time, Type, Virus Name, File Name, Action Taken, Mode, and E-mail Info columns.
Firewall	Displays the Rating, Date/Time, Type, Protocol, Program, Source IP, Destination IP, Direction, Action Taken, Count, Source DNS, and Destination DNS columns.
OSFirewall	Displays the Rating, Date/Time, Type, Subtype, Data, Program, Direction, Action Taken, and Count columns.
Program	Displays the Rating, Date/Time, Type, Program, Source IP, Destination IP, Direction, Action Taken, Count, Source DNS, and Destination DNS columns.
Spy Site Blocking	Displays the Date/Time and the site that was blocked.

The Log Viewer shows security events that have been recorded in the ZoneAlarm security software log. To view details of Log Viewer fields for each alert type, refer to the Firewall, Program Control, and Anti-virus chapters.

Field	Information
Description	A description of the event.
Direction	The direction of the blocked traffic. “Incoming” means the traffic was sent to your computer. “Outgoing” means the traffic was sent from your computer.
Type	The type of alert: Firewall, Program, ID Lock, or Lock Enabled.

Table 12-1: Log viewer fields

Field	Information
Source DNS	The domain name of the computer that sent the traffic that caused the alert.
Source IP	The IP address of the computer that sent the traffic that ZoneAlarm security software blocked.
Rating	Each alert is high-rated or medium-rated. High-rated alerts are those likely to have been caused by hacker activity. Medium-rated alerts are likely to have been caused by unwanted but harmless network traffic.
Protocol	The communications protocol used by the traffic that caused the alert.
Action Taken	How the traffic was handled by ZoneAlarm security software.
Destination DNS	The domain name of the intended addressee of the traffic that caused the alert.
Destination IP	The address of the computer the blocked traffic was sent to.
Count	The number of times an alert of the same type, with the same source, destination, and protocol, occurred during a single session.
Date/Time	The date and time the alert occurred.
Program	The name of the program attempting to send or receive data. (Applies only to Program and ID Lock alerts).

Table 12-1: Log viewer fields

Viewing the text log

By default, alerts generated by ZoneAlarm security software are logged in the file, *ZAlog.txt*. If you are using Windows95, Windows98 or Windows Me, the file is located in the following folder: (x):\Windows\Internet Logs. If you are using WindowsNT or Windows2000, the file is located in the following folder: (x):\Winnt\Internet Logs.

To view the current log as a text file:

1. Select **Alerts & Logs**.
2. Click **Advanced**.

   The Advanced Alerts & Log Settings dialog box opens.
3. Select the **Log Control** panel.

In the Log Archive Location area, click **View Log**.

Text log fields

Log entries contain some combination of the fields described in the table below.

Field	Description	Example
Type	The type of event recorded.	FWIN
Date	The date of the alert, in format yyyy/mm/dd	2001/12/31(December 31, 2001)
Time	The local time of the alert. This field also displays the hours difference between local and Greenwich Mean Time (GMT).	17:48:00 -8:00GMT (5:48 PM, eight hours earlier than Greenwich Mean Time. GMT would be 01:48.)
Virus Name	The name of the virus that caused the event. This field only appears for anti-virus events.	iloveyou
File name	The name of the file that caused the event. This field only appears for Anti-virus events.	iloveyou.exe
Action	How the event was handled. The value for this field will depend on the type of event that occurred.	Anti-virus: Renamed MailSafe: Quarantined ID Lock: Blocked
Category	The ID Lock category of information that was detected in the event. This field only appears for ID Lock events.	Access PIN
Program	The program sending or receiving the e-mail that contains the ID Lock information. This field only appears for ID Lock events.	Outlook.exe
Source	The IP address of the computer that sent the blocked packet, and the port used; OR the program on your computer that requested access permission.	192.168.1.1:7138 Outlook.exe
Destination	The IP address and port of the computer the blocked packet was addressed to.	192.168.1.101:0

Field	Description	Example
Transport	The protocol (packet type) involved.	UDP

Archiving log entries

At regular intervals, the contents of ZAlog.txt are archived to a date-stamped file, for example, ZALog2004.06.04.txt (for June 4, 2004). This prevents ZAlog.txt from becoming too large.

To view archived log files, use Windows Explorer to browse to the directory where your logs are stored.

To set archive frequency:

1. Select **Alerts & Logs**, then click **Advanced**.
2. Select the **Log Control** panel.
3. Select the **Log Archive Frequency** check box.

If the Log Archive Frequency check box is not selected, ZoneAlarm security software continues to log events for display in the Log Viewer panel, but does not archive them to the ZAlog.txt file.

4. In the Log Frequency area, specify the log frequency (between 1 and 60 days), then click **Apply**.

Specifying the archive location

The ZAlog.txt file and all archived log files are stored in the same directory.

To change the log and archive location:

1. Select **Alerts & Logs**.
2. Click **Advanced**.

   The Advanced Alerts & Log Settings dialog box opens.
3. Select the **Log Control** panel.
4. In the Log Archive Location area, click **Browse**.

   Select a location for the log and archive files.

Using SmartDefense Advisor and Hacker ID

ZoneAlarm SmartDefense Advisor is a service that enables you to instantly analyze the possible causes of an alert, and helps you decide how to respond. When available, SmartDefense Advisor provides advice as to how to respond to Program alerts. If no advice is available, click **More Info** in the alert to receive more information about the alert. SmartDefense Advisor returns an article that explains the alert and gives you advice on what, if anything, you need to do to ensure your security.

To determine the physical location and other information about the source IP address or destination IP address in an alert, click the Hacker ID panel. This panel displays available information about the IP address that was submitted.

If you are a frequent visitor to eBay, and you have received an ID Lock alert blocking your eBay password, you can use SmartDefense Advisor to submit a fraud report to eBay. To learn more about how ZoneAlarm security software protects your eBay identity, see "Creating an online fraud protection profile," on page 17.

To submit an alert to SmartDefense Advisor:

1. Select **Alerts & Logs | Log Viewer**.
2. Right-click anywhere in the alert record you want to submit.
3. Select **More Info** from the shortcut menu.

Chapter 13

Game Mode

Game Mode temporarily suppresses most ZoneAlarm security software scans, product updates, and alerts, so that you can play games on your computer with fewer interruptions.

Topics:

- Understanding Game Mode
- Turning Game Mode On and Off

Understanding Game Mode

Game Mode minimizes interruptions while you play computer games by doing the following:

- Lets you temporarily allow or deny all program permission requests, so that requests are answered without displaying alerts.
- Postpones automatic scans and product updates.
- Suppresses all Informational alerts and all alerts in which you are prompted to make a decision. This includes:
  - Alerts caused by Ask settings in the Programs List, such as permission alerts triggered by programs trying to send mail or act as servers.
  - OSFirewall alerts, which prompt you to allow or deny behavior considered unusual or suspicious.
  - ID Lock alerts and Outbound Mailsafe alerts.

Game Mode settings do not override Block or Allow settings in your Programs List. If you have configured ZoneAlarm security software to always block a specific program, it

continues to block that program even if you activate Game Mode with a setting of Allow.

Game Mode remains active until you turn it off, or until you turn off ZoneAlarm security software or your computer.

See "Turning Game Mode On and Off," on page 194.

Turning Game Mode On and Off

To turn Game Mode on:

1. Do one of the following:
   - Right-click the system tray icon, and choose **Game Mode...**
   - Or, under **QuickTasks,** click **Set Gaming**.
2. In the dialog that appears, choose one of the following:

   Answer all alerts with "allow"—Permission requests will be granted.

   Answer all alerts with "deny"—Permission requests will be denied.

   See "Understanding Game Mode," on page 193 for more information.

The use of Game Mode may reduce the security of your system. If you choose to allow all permission requests, you may increase the chances of a malicious program harming your computer or gaining access to your data. If, on the other hand, you choose to deny all requests, you may interrupt the functions of a legitimate program.

You should activate Game Mode only for the duration of your game.

3. Leave the Activate Game Mode dialog open or minimize it, but do not close it.

If you close the Activate Game Mode dialog, you turn Game Mode off.

While Game Mode is on, ZoneAlarm security software displays a special icon in the system tray ( ).

To turn Game Mode off:

Do one of the following:

- Close the Activate Game Mode dialog by clicking either **Cancel** or the Close icon (x) at upper right.
- Click **Stop Game Mode** in the Activate Game Mode dialog.
- Right-click the system tray icon and choose **Stop Game Mode**.

Note that Game Mode is automatically deactivated if you turn off your computer or if you turn off ZoneAlarm security software.

Appendix

Troubleshooting

14

This chapter provides guidance for troubleshooting issues you may encounter while using ZoneAlarm security software.

Topics:

- "VPN," on page 197
- "Networking," on page 199
- "Internet Connection," on page 200
- "Anti-virus," on page 203
- "Hard Drive Encryption," on page 205
- "Third-party software," on page 205

VPN

If you are having difficulty using VPN software with ZoneAlarm security software, refer to the table for troubleshooting tips provided in this section.

If...	See...
You can't connect to your Virtual Private Network (VPN)	"Configuring ZoneAlarm security software for VPN traffic," on page 198
You have created expert firewall rules	"VPN auto-configuration and expert rules," on page 198

Table 14-1: Troubleshooting VPN problems

If...	See...
You are using a supported VPN client and ZoneAlarm security software does not detect it automatically the first time you connect	"Automatic VPN detection delay," on page 198

Table 14-1: Troubleshooting VPN problems

Configuring ZoneAlarm security software for VPN traffic

If you cannot connect to your VPN, you may need to configure ZoneAlarm security software to accept traffic coming from your VPN.

To configure ZoneAlarm security software to allow VPN traffic:

1. Add VPN-related network resources to the Trusted Zone.

   See "Adding to the Trusted Zone," on page 40.

2. Grant access permission to the VPN client and any other VPN-related programs on your computer.

   See "Setting permissions for specific programs," on page 101.

3. Allow VPN protocols.

   See "Adding a VPN gateway and other resources to the Trusted Zone," on page 30.

VPN auto-configuration and expert rules

If you have created expert firewall rules that block VPN protocols, ZoneAlarm security software will not be able to automatically detect your VPN when you initiate a connection. To configure your VPN connection, you will need to make sure that your VPN client and VPN-related components are in the Trusted Zone, and that they have permission to access the Internet. See "Configuring your VPN connection," on page 27.

Automatic VPN detection delay

ZoneAlarm security software periodically polls your computer to determine if supported VPN protocols are engaged. Upon detection, ZoneAlarm security software prompts you to configure your connection automatically. If you have recently install a VPN client and have tried to connect, ZoneAlarm security software may not have detected your VPN configuration. If you prefer ZoneAlarm security software to configure your connection automatically, you can wait ten minutes then, try connecting again. If you prefer to connect right away, you can configure your connection manually. See "Configuring your VPN connection," on page 27.

Networking

If you are having difficulty connecting to your network or using networking services, refer to the table for troubleshooting tips provided in this section.

If ...	See...
You can't see the other computers in your Network Neighborhood, or if they can't see you	"Making your computer visible on your local network," on page 199
You can't share files or printers over your home or local network	"Sharing files and printers across a local network," on page 199
Your computer is on a Local Area Network (LAN) and takes a long time to start up when ZoneAlarm security software is installed	"Resolving a slow start up," on page 200

Table 14-2: Troubleshooting network problems

Making your computer visible on your local network

If you can't see the other computers on your local network, or if they can't see your computer, it is possible that ZoneAlarm security software is blocking the NetBIOS traffic necessary for Windows network visibility.

To make your computer visible on the local network:

1. Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone. See "Adding to the Trusted Zone," on page 40.
2. Set the Trusted Zone security level to Medium, and the Internet Zone security level to High. This allows trusted computers to access your shared files, but blocks all other machines from accessing them. See "Setting advanced security options," on page 35.

ZoneAlarm security software will detect your network automatically and display the New Network alert. You can use the alert to add your network subnet to the Trusted Zone. For more information, see "New Network alerts," on page 83.

Sharing files and printers across a local network

ZoneAlarm security software enables you to quickly and easily share your computer so that the trusted computers you're networked with can access your shared resources, but Internet intruders can't use your shares to compromise your system.

To configure ZoneAlarm security software for secure sharing:

1. Add the network subnet (or, in a small network, the IP address of each computer you're sharing with) to your Trusted Zone. See "Adding to the Trusted Zone," on page 40.
2. Set the Trusted Zone security level to Medium. This allows trusted computers to access your shared files. See "Choosing security levels," on page 34.
3. Set the Internet Zone security level to High. This makes your computer invisible to non-trusted computers. See "Setting the security level for a Zone," on page 34.

Resolving a slow start up

If ZoneAlarm security software is configured to load at startup, some users connected to the LAN may find that it takes several minutes for the startup process to finish.

In most cases, this is because your computer needs access to your network's Domain Controller to complete its startup and login process, and ZoneAlarm security software is blocking access because the Controller has not been added to the Trusted Zone.

To solve this problem, add the host name or IP address of your network's Domain Controller to the Trusted Zone.

Internet Connection

If you are having difficulty connecting to the Internet, refer to the table for troubleshooting tips provided in this section.

If...	See...
You cannot connect to the Internet	"Connecting to the Internet fails after installation," on page 201
You can connect to the Internet but are disconnected after a short time	"Allowing ISP Heartbeat messages," on page 201
Your computer is an Internet Connection Sharing (ICS) client and you can't connect to the Internet	"Connecting through an ICS client," on page 202
Your computer uses a proxy server to connect to the Internet and you can't connect to the Internet	"Connecting through a proxy server," on page 202
You see the message "Could not contact automatic program server" in a program alert.	"Unable to connect to program advice server," on page 202

Table 14-3: Troubleshooting Internet connection problems

Connecting to the Internet fails after installation

If you are unable to connect to the Internet after installing ZoneAlarm security software, the first troubleshooting step is to determine whether ZoneAlarm security software is the cause. If you are unable to follow the steps below, for example, if you can't clear the **Load ZoneAlarm security software at startup** check box, contact ZoneAlarm technical support.

To determine if ZoneAlarm security software is the cause of connection problems:

1. Select **Overview | Preferences**.
2. In the General area, clear the check box **Load ZoneAlarm security software at startup**.

   A warning dialog labeled ZoneAlarm TrueVector Service opens.
3. Click **Allow**.
4. Restart your computer, then try to connect to the Internet.

If you can connect	Your ZoneAlarm security software settings may be the cause of your connection problems. Make sure that your browser has access permission.
If you cannot connect	Your ZoneAlarm security software settings are not the cause of your connection problems.

Allowing ISP Heartbeat messages

Internet Service Providers (ISPs) periodically send heartbeat messages to their connected dial-up customers to make sure they are still there. If the ISP cannot determine that the customer is there, it might disconnect the customer so that the user's IP address can be given to someone else.

By default, ZoneAlarm security software blocks the protocols most commonly used for these heartbeat messages, which may cause you to be disconnected from the Internet. To prevent this from happening, you can identify the server sending the messages and add it to your Trusted Zone or you can configure the Internet Zone to allow ping messages.

Identifying the source of the heartbeat messages

This is the preferred solution because it will work whether your ISP uses NetBIOS or *ICMP (Internet Control Message Protocol)* to check your connection, and it allows you to maintain high security for the Internet Zone.

To identify the server your ISP uses to check your connection:

1. When your ISP disconnects you, click **Alerts & Logs | Log Viewer**.
2. In the alerts list, find the alert that occurred at the time you were disconnected.

3. In the Entry Detail area, note the Source DNS detected.

   If you're not able to identify the server this way, contact your ISP to determine which servers need access permission.

4. After you have identified the server, add it to the Trusted Zone.

   See "Adding to the Trusted Zone," on page 40.

Configuring ZoneAlarm security software to allow ping messages

If your ISP uses ICMP echo (or ping) messages for connectivity checks, configure ZoneAlarm security software to allow ping messages from the Internet Zone.

To configure ZoneAlarm security software to allow ping messages:

1. Select **Firewall**.
2. In the Internet Zone area, click **Custom**.
3. Select check box labeled **Allow incoming ping (ICMP echo)**.
4. Click **OK**.
5. Set the security level for the Internet Zone to Medium.

   See "Choosing security levels," on page 34.

Connecting through an ICS client

If you are using Windows' Internet Connection Sharing (ICS) option, or a third-party connection sharing program, and you are unable to connect to the Internet, make sure that ZoneAlarm security software is properly configured for the client and gateway machines. See "Enabling Internet Connection Sharing," on page 27.

Do not configure ZoneAlarm security software for Internet Connection Sharing if you use hardware such as a server or router, rather than a host PC.

Connecting through a proxy server

If you connect to the Internet through a proxy server and you are unable to connect to the Internet, make sure that the IP address of your proxy server is in your Trusted Zone. See "Adding to the Trusted Zone," on page 40.

Unable to connect to program advice server

If you receive a Program alert with the message "Could not contact automatic program server," in the SmartDefense Advisor area, make sure that your Internet Connection is working properly.

- Verify that your computer is connected to the network or modem properly.
- If you are connected to the Internet via cable modem or DSL, you may have encountered a temporary service interruption.

- Many times it is just a matter of trying again later if the user has a working configuration.
- Launch your browser. If you are unable to connect to any site on the Internet, you may have ZoneAlarm security software configured to block Internet access. Providing the correct permission to your browser may resolve the problem.

If none of these scenarios apply, it's possible that the server is temporarily unavailable.

Anti-virus

If you are having difficulty connecting using anti-virus software refer to the table for troubleshooting tips provided in this section.

If...	See...
An application you trust has been quarantined.	"If a safe application has been quarantined," on page 203
Anti-virus Monitoring feature is unavailable	"Anti-virus Monitoring alert," on page 204
You receive an alert about conflicting products	"Resolving conflicts with anti-virus products," on page 204
You are unable to turn on the Anti-virus feature	"E-mail scanning is unavailable," on page 204

Table 14-4: Troubleshooting ZoneAlarm Anti-virus problems

If a safe application has been quarantined

On rare occasions, it's possible that an application you trust is quarantined because it is a spoof of the real application and therefore was detected as a virus. But, if an application that you know to be safe is quarantined, it may be a false positive virus detection. False positives occur when a pattern of code in the file matches the same pattern contained in a virus signature. This can occur due to a faulty signature or it can occur after incomplete treatment by another anti-virus scanner. False positives are most likely to occur in applications that are not widely used.

If you believe your application has been improperly quarantined, here's how to restore it and stop putting it in quarantine:

1. Select **Anti-virus | Quarantine**.
2. Select your item under **Quarantine** and click the **Restore** button.
3. Select **Anti-virus/spyware**, then click **Advanced Options.**
4. Under **Virus Management**, click **Exceptions**.

5. Click **Add file...** and browse to select the trusted program that you do not want quarantined in a virus scan.
6. Click **OK** to close Add File and then to close Advanced Options.

If the above technique does not work for your program:
Select **Anti-virus/spyware**, then click **Advanced Options**. Under Virus Management, select **Automatic Treatment**, and select **Alert me - do not treat automatically**. Then try the steps above again. Be sure to go back and restore the Automatic Treatment setting afterward.

You can send names of suspected false positive detections to spywarefeedback@checkpoint.com.

Anti-virus Monitoring alert

The Anti-virus Monitoring alert lets you know when the anti-virus protection on your computer is not fully protecting you from viruses. You may receive this alert when your anti-virus is turned off, when your anti-virus signatures are not up-to-date, or when you are not running any anti-virus software at all.

Note that not all anti-virus products are monitored, so the absence of an alert does not necessarily mean you are protected. To ensure your protection, open your anti-virus software (if it is installed) and perform an update or renew your subscription, if it has expired.

Resolving conflicts with anti-virus products

If you also have another anti-virus product installed, you may receive a conflict alert that states you must uninstall that product before using ZoneAlarm anti-virus. The alert will list the anti-virus software products that were detected and specify whether ZoneAlarm is able to uninstall them automatically, or if they must be uninstalled manually. If the products listed cannot be uninstalled automatically, refer to the individual vendor's documentation for instructions for uninstalling the products.

E-mail scanning is unavailable

If you are attempting to enable the e-mail scanning option of ZoneAlarm anti-virus software and are unable to do so, you may have a product installed that uses Layered Service Provider (LSP) technology that is incompatible with ZoneAlarm. To remedy this situation, you will need to uninstall the conflicting product(s).

When a conflict occurs, a file called lspconflict.txt is created and placed in the C:/Windows/Internet Logs directory. This file contains the name of the product(s) that caused the conflict. You can remove the product(s) manually or send e-mail to **lspsupport@zonealarm.com** and attach the file. Refer to the individual vendors' documentation for instructions for uninstalling the product(s).

Hard Drive Encryption

For troubleshooting the *Hard Drive Encryption* feature, refer to the table below.

If...	See...
You forgot your password or username	"What to do if you forget your password or username:," on page 178
Your system crashes and you need to recover the disk but it is encrypted	"How to decrypt in case of system failure," on page 178

Table 14-5: Troubleshooting Hard Drive Encryption problems

Third-party software

Many of your most commonly used programs can be configured automatically for Internet access. Although, in some cases, Internet access can be configured automatically, many programs also require server access rights.

If you are using programs that ZoneAlarm security software is unable to recognize and configure automatically, you may need to configure permissions manually. Refer to the sections that follow to learn how to configure your programs for use with ZoneAlarm security software.

- Anti-virus
- Browsers
- Chat and instant messaging programs
- E-mail programs
- Internet answering machine programs
- File sharing programs
- FTP programs
- Games
- Remote control programs
- VNC programs
- Streaming media programs
- Voice over IP programs
- Web conferencing programs

Anti-virus

In order for your anti-virus software to receive updates it must have access permission for the Trusted Zone.

Automatic updates

In order to receive automatic updates from your anti-virus software vendor, add the domain that contains the updates (e.g., update.avsupdate.com) to your Trusted Zone. See "Adding to the Trusted Zone," on page 40.

Browsers

In order for your browser to work properly, it must have access permission for the Internet Zone and Trusted Zone. Before granting permission, make sure that you understand how to configure your browser's security for optimal protection and have the latest service packs installed for the browser you are using.

To grant your browser access permission, do any of the following:

- Grant access to the program directly. See "Granting a program permission to access the Internet," on page 106.
- Select **Allow** when a Program alert for the browser appears.

Internet Explorer

You may need to allow Internet access rights to the Services and Controller App (the file name is typically services.exe).

To grant Internet access permission to the Services and Controller App:

1. Select **Program Control**|**Programs**.
2. In the Programs column, locate **Services and Controller App**.
3. In the Access column, select **Allow** from the shortcut menu.

Chat and instant messaging programs

Chat and instant messaging programs (for example, AOL Instant Messenger) may require server permission in order to operate properly.

To grant server permission to your chat program:

- Answer Allow to the Server Program alert caused by the program.
- Grant server permission to the program.

See "Granting a program permission to act as a server," on page 106.

We strongly recommend that you set your chat software to refuse file transfers without prompting first. File transfer within chat programs is a means to distribute malware such as worms, viruses, and Trojan horses. Refer to your chat software vendor's help files to learn how to configure your program for maximum security.

E-mail programs

In order for your e-mail program (for example, Microsoft Outlook) to send and receive mail, it must have access permission for the Zone the mail server is in. In addition, some e-mail client software may have more than one component requiring server permission. For example, Microsoft Outlook requires that both the base application (OUTLOOK.EXE) and the Messaging Subsystem Spooler (MAPISP32.exe) to have server permission.

While you can give your e-mail program access to the Internet Zone, and leave the mail server there, it's safer to place the mail server in the Trusted Zone, and limit the program's access to that Zone only. Once your e-mail client has access to the Trusted Zone, add the remote mail server (host) to the Trusted Zone.

To learn how to give a program permission to access or act as a server to the Trusted Zone, see "Setting program permissions manually," on page 91.

To learn how to add a host to the Trusted Zone, see "Managing traffic sources," on page 39.

Internet answering machine programs

To use Internet answering machine programs (such as CallWave) with ZoneAlarm security software, do the following:

- Give the program server permission and access permission for the Internet Zone.
- Add the IP address of the vendor's servers to the Trusted Zone.

To find the server IP address, contact the vendor's technical support.

- Set the security level for the Internet Zone to Med.

File sharing programs

File sharing programs, such as Napster, Limewire, AudioGalaxy, or any Gnutella client software, must have server permission for the Internet Zone in order to work with ZoneAlarm security software.

FTP programs

To use FTP (File Transfer Protocol) programs, you may need to make the following settings adjustments in your FTP client program and in ZoneAlarm security software:

- Enable passive or PASV mode in your FTP client

  This tells the client to use the same port for communication in both directions. If PASV is not enabled, ZoneAlarm security software may block the FTP server's attempt to contact a new port for data transfer.

- Add the FTP sites you use to the Trusted Zone
- Give Trusted Zone access permission to your FTP client program.

To learn how to add to the Trusted Zone and give access permission to a program, see "Setting advanced security options," on page 35.

Games

In order to play games over the Internet while using ZoneAlarm security software, you may have to adjust the settings listed below.

Note that you can configure ZoneAlarm security software to suppress most alerts while you are playing a game. For details, see "Game Mode," on page 193.

Program permission

In order to function, many Internet games require access permission and/or server permission for the Internet Zone.

The easiest way to grant access is to answer "Allow" to the program alert caused by the game program. However, many games run in "exclusive" full screen mode, which will prevent you from seeing the alert. Use any of the methods below to solve this problem.

- Set the game to run in a window

  This will allow you to see the alert, if the game is running at a resolution lower than that of your desktop. If the alert appears but you cannot respond to it because your mouse is locked to the game, press the Windows logo key on your keyboard.

  After granting the game program Internet access, reset the game to run full-screen.

- Use software rendering mode

  By changing your rendering mode to "Software Rendering," you can allow Windows to display the alert on top of your game screen. After allowing the game Internet access, you can change back to your preferred rendering device.

- Use Alt+Tab

Press **Alt+Tab** to toggle back into Windows. This leaves the game running, but allows you to respond to the alert. Once you have allowed Internet access, press **Alt+Tab** again to restore your game.

The last method may cause some applications to crash, especially if you are using Glide or OpenGL; however, the problem should be corrected the next time you run the game. Sometimes you can use Alt-Enter in the place of Alt-Tab.

Security level/Zone

Some Internet games, particularly those that use Java, applets, or other Web-based portal functionality, may not work properly when your Internet Zone security level is set to High. High security will also prevent remote game servers from "seeing" your computer. To solve these problems, you can:

- Change your Internet Zone security level to Medium, or
- Add the IP address of the game server you're connecting to the Trusted Zone. The game manufacturer's documentation should indicate the IP address or host name of the server.

To learn how to add a host or IP address to the Trusted Zone, see "Adding to the Trusted Zone," on page 40.

Trusting game servers means trusting the other players in the game. ZoneAlarm security software does not protect you from attacks instigated by fellow gamers in a trusted environment. Make sure that you understand how to configure your browser's security for optimal protection and have the latest service packs installed for the browser you are using.

Remote control programs

If your computer is either the host or the client of a remote access system such as PCAnywhere or Timbuktu:

- Add the IP address(es) of the hosts or clients to which you connect to your Trusted Zone. See "Adding to the Trusted Zone," on page 40.
- Add the subnet of the network you are accessing remotely to your Trusted Zone. See "Adding to the Trusted Zone," on page 40.

- If a dynamic IP address is assigned to the remote machine, add the DHCP server address or range of addresses to the Trusted Zone.

If your remote control client or host is on a network not under your control (for example on a business or university LAN), perimeter firewalls or other features of the network may prevent you from connecting. If you still have problems connecting after following the instructions above, contact your network administrator for assistance.

VNC programs

In order for VNC and ZoneAlarm security software to work together, follow the steps below.

1. On both the server and viewer (client) machine, do one of the following:

   - If you know the IP address or subnet of the viewer (client) you will be using for remote access, and it will always be the same, add that IP or subnet to the Trusted Zone. See "Adding to the Trusted Zone," on page 40.

     If you do not know the IP address of the viewer, or if it will change, then give the program access permission and server permission for the Trusted and Internet Zones. See "Setting permissions for specific programs," on page 101.

     When prompted by VNC Viewer on the viewer machine, enter the name or IP address of the server machine, followed by the password when prompted. You should be able to connect.

If you enable VNC access by giving it server permission and access permission, be sure to set and use your VNC password in order to maintain security. We recommend adding the server and viewer IP addresses to the Trusted Zone, rather than giving the application Internet Zone permission, if possible.

2. On the viewer (client) machine, run VNC Viewer to connect to the server machine. Do not run in "listen mode."

Telnet

To access a remote server via Telnet, add the IP address of that server to your Trusted Zone.

Streaming media programs

Applications that stream audio and video, such as RealPlayer, Windows Media Player, QuickTime, etc., must have server permission for the Internet Zone in order to work with ZoneAlarm security software.

To learn how to give server permission to a program, see "Granting a program permission to act as a server," on page 106.

Voice over IP programs

To use Voice over IP (VoIP) programs with ZoneAlarm security software, you must do one or both of the following, depending on the program:

1. Give the VoIP application server permission and access permission.
2. Add the VoIP provider's servers to the Trusted Zone. To learn the IP addresses of these servers, contact your VoIP provider's customer support.

Web conferencing programs

If you experience problems using a Web conferencing program such as Microsoft NetMeeting, try the following:

1. Add the domain or IP address that you connect to in order to hold the conference to the Trusted Zone. See "Adding to the Trusted Zone," on page 40.
2. Disable the conferencing program's "Remote Desktop Sharing" option.

Appendix

Keyboard shortcuts

A

Many features of ZoneAlarm security software are accessible using keyboard shortcuts.

- "Navigation shortcuts," on page 215
- "Global function shortcuts," on page 216
- "Dialog box commands," on page 217
- "Button shortcuts," on page 218

Navigation shortcuts

Use these keystrokes to navigate through panels, settings, and dialog boxes. Use UP, DOWN, LEFT, and RIGHT arrows to reach the selection you want within that group.

Keystroke	Function
F1	Opens online help for the current panel.
UP and DOWN arrows	Navigates through individual controls within a group of controls.
LEFT and RIGHT arrows	Also navigate through individual controls within a group of controls. In list views, controls horizontal scrolling.

Table A-1: Navigation shortcuts

Keystroke	Function
ALT+SPACEBAR	Opens the Windows control menu (maximize, minimize, close).

Table A-1: Navigation shortcuts

Global function shortcuts

Use the following keystrokes to activate functions from multiple locations in the interface. Note that some keystrokes may have other functions in specific panels. Those cases are listed under Button Shortcuts, below.

Keystroke	Function
ALT+C	Opens a Custom dialog box, where one is available.
ALT+U	Opens a second Custom dialog box, where two Custom buttons are available (for example, in the main panel of the Program Control panel).
ALT+A	Opens an advanced dialog box, where one is available.
ALT+DOWN ARROW	Opens the active drop-down list box. In list views, opens the left-click shortcut menu if one is available.
SHIFT+F10	In list views, opens the right-click shortcut menu if one is available.
ESC	Equivalent to clicking a Cancel button.
ENTER	Equivalent to clicking the active button.
ALT+P	Equivalent to clicking an Apply button.
Delete	Removes a selected item from a list view.

Table A-2: Global shortcuts

Keystroke	Function
ALT+F4	Shuts down ZoneAlarm security software.

Table A-2: Global shortcuts

Dialog box commands

Use the keystrokes below when a dialog box is open.

Keystroke	Function
Tab	Activates the next control in the dialog box.
SHIFT+TAB	Activates the previous control in the dialog box.
CTRL+TAB	Opens the next TAB in a multiple-TAB dialog box.
CTRL+SHIFT+TAB	Opens the previous TAB in a multiple-TAB dialog box.
ALT+DOWN ARROW	Opens the active drop-down list box.
SPACEBAR	Clicks an active button. Selects/clears an active check box.
ENTER	Same as clicking the active button
ESC	Same as clicking the Cancel button.

Table A-3: Dialog box shortcuts

Button shortcuts

Use the keystrokes below to click available buttons in an active window.

Panel	Pane	Keystroke	Equivalent to clicking
Overview	Product Info	Alt + I	Change License
Overview	Product Info	Alt + B	Buy Now
Overview	Product Info	Alt + N	Renew
Overview	Product Info	Alt + R	Change Reg.
Overview	Preferences	Alt + P	Set Password
Overview	Preferences	Alt + B	Backup
Overview	Preferences	Alt + R	Restore
Overview	Preferences	Alt + O	Log In/Log Out
Overview	Preferences	Alt + U	Check for Update
Firewall	Main	Alt + C	Internet Zone Custom
Firewall	Main	Alt + U	Trusted Zone Custom

Table A-4: Keystrokes for activating buttons

Panel	Pane	Keystroke	Equivalent to clicking
Firewall	Main	Alt + A	Advanced
Firewall	Zones	Alt +A	Add
Firewall	Zones	Alt + R	Remove
Firewall	Zones	Alt + E	Edit
Firewall	Zones	Alt + P	Apply
Firewall	Expert	Alt + A	Add
Firewall	Expert	Alt + R	Remove
Firewall	Expert	Alt + E	Edit
Firewall	Expert	Alt + P	Apply
Firewall	Expert	Alt + G	Groups
Program Control	Main	Alt + C	Program Control Custom
Program Control	Main	Alt + U	Automatic Lock Custom
Program Control	Main	Alt + A	Advanced
Program Control	Programs	Alt + A	Add
Program Control	Programs	Alt + O	Options
Program Control	Components	Alt + M	More info
Anti-virus / Anti-spyware	Main	ALT + S	Scan for Viruses/Spyware
Anti-virus / Anti-spyware	Main	ALT + U	Update Now
Anti-virus / Anti-spyware	Main	ALT + A	Advanced Options
Anti-virus / Anti-spyware	Main	ALT + V	Scan for Viruses
Anti-virus / Anti-spyware	Quarantine	ALT + D	Delete
Anti-virus / Anti-spyware	Quarantine	ALT + E	Restore
Anti-virus / Anti-spyware	Quarantine	ALT + M	More Info
E-mail Protection	Main	ALT + A	Advanced
E-mail Protection	Attachments	ALT + C	Check All
E-mail Protection	Attachments	ALT + R	Clear All
E-mail Protection	Attachments	ALT + A	Add
E-mail Protection	Attachments	ALT + P	Apply
ID Lock	myVAULT	Alt + A	Add
ID Lock	myVAULT	Alt + O	Options
ID Lock	myVAULT	Alt + N	Encrypt
ID Lock	myVAULT	Alt + E	Edit
ID Lock	myVAULT	Alt + R	Remove

Table A-4: Keystrokes for activating buttons

Panel	Pane	Keystroke	Equivalent to clicking
ID Lock	Trusted Sites	Alt + A	Add
ID Lock	Trusted Sites	Alt + R	Remove
Parental Control	Main	Alt + A	Advanced
Parental Control	Categories	Alt + C	Check All
Parental Control	Categories	Alt + R	Clear All
Alerts & Logs	Main	Alt + D	Reset to Default
Alerts & Logs	Main	Alt + C	Custom
Alerts & Logs	Main	Alt + A	Advanced
Alerts & Logs	Log Viewer	Alt + M	More Info
Alerts & Logs	Log Viewer	Alt + D	Clear List
Alerts & Logs	Log Viewer	Alt + A	Add to Zone
Alerts & Logs	Log Control	Alt + B	Browse
Alerts & Logs	Log Control	Alt + E	Delete Log

Table A-4: Keystrokes for activating buttons

Glossary

1394
A very fast external bus standard that supports data transfer rates of up to 400Mbps (in 1394a) and 800Mbps (in 1394b). Products supporting the 1394 standard go under different names, depending on the company. Apple, which originally developed the technology, uses the trademarked name FireWire.

3DES
Short for Triple Data Encryption Standard, a standards-based symmetric-key encryption method using a 168-bit key. 3DES is a more robust variation of the older 56-bit DES encryption standard.

ACCESS PERMISSION
Access permission allows a program on your computer to initiate communications with another computer. This is distinct from server permission, which allows a program to "listen" for connection requests from other computers. You can give a program access permission for the Trusted Zone, the Internet Zone, or both.

ACT AS A SERVER
A program acts as a server when it "listens" for connection requests from other computers. Several common types of applications, such as chat programs, e-mail clients, and Internet Call Waiting programs, may need to act as servers to operate properly. However, some hacker programs act as servers to listen for instructions from their creators. ZoneAlarm security software prevents programs on your computer from acting as servers unless you grant server permission.

ACTIVEX CONTROLS
A set of technologies developed by Microsoft that can be automatically downloaded and executed by a Web browser. Because ActiveX controls have full access to the Windows operating system, they have the potential to damage software or data on a user's machine.

AD BLOCKING
A ZoneAlarm security software feature that enables you to block banner, pop-up and other types of advertisements.

ADVANCED PROGRAM CONTROL
Advanced Program Control is an advanced security feature that tightens your security by preventing unknown programs from using trusted programs to

access the Internet.

ANIMATED AD
An advertisement that incorporates moving images.

BANNER AD
An ad that appears in a horizontal banner across a Web page.

BLOCKED ZONE
The Blocked Zone contains computers you want no contact with. ZoneAlarm security software prevents any communication between your computer and the machines in this Zone.

BLUE COAT
Blue Coat is a software development and application services company that filters, monitors and reports on Internet use and activity. The Parental Control feature uses Blue Coat content categories to determine whether access to Web sites you visit will be allowed or blocked.

BOOT SECTOR VIRUS
Type of computer virus that infects the first or first few sectors of a computer hard drive or diskette drive allowing the virus to activate as the drive or diskette boots.

CACHE CLEANER
Privacy feature that enables you to remove unwanted files and cookies from your computer on demand, or on a scheduled basis.

CLEAR TEXT
Clear text, also referred to as "plain text," is data that is being transmitted in textual form and is not encrypted. Because the data is not encrypted, it could be intercepted and read by others during transmission.

COLLABORATIVE FILTER
A feature of Zone Labs security software's junk e-mail filter. Collaborative filtering uses information extracted from junk e-mail reported by you and other ZoneAlarm security software users to determine the probability that new messages from unknown senders are spam.

COMPONENT
A small program or set of functions that larger programs call on to perform specific tasks. Some components may be used by several different programs simultaneously. Windows operating systems provide many component DLLs (Dynamic Link Libraries) for use by a variety of Windows applications.

COMPONENT LEARNING MODE
The period after installation when program control is set to Medium. When in component learning mode, ZoneAlarm security software can quickly learn the MD5 signatures of many frequently used components without interrupting

your work with multiple alerts.

COOKIE

A small data file used by a Web site to customize content, remember you from one visit to the next, and/or track your Internet activity. While there are many benign uses of cookies, some cookies can be used to divulge information about you without your consent.

DES

Short for Data Encryption Standard, a popular symmetric-key encryption method using a 56-bit key. DES has been supplanted by 3DES, a more robust variation of DES.

DESTRUCTIVENESS

Refers to the extent of the damage caused by a virus. The Destructiveness rating refers to the degree to which the damage can be reversed. A low Destructiveness rating would indicate that the scale of the interruption was small, and that any damage done could be reversed. A Medium or High Destructiveness rating would indicate that the damage caused may be irreversible, or that it caused a widespread interruption.

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

A protocol used to support dynamic IP addressing. Rather than giving you a static IP address, your ISP may assign a different IP address to you each time you log on. This allows the provider to serve a large number of customers with a relatively small number of IP addresses.

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) BROADCAST/MULTICAST

A type of message used by a client computer on a network that uses dynamic IP addressing. When the computer comes online, if it needs an IP address, it issues a broadcast message to any DHCP servers which are on the network. When a DHCP server receives the broadcast, it assigns an IP address to the computer.

DIAL-UP CONNECTION

Connection to the Internet using a modem and an analog telephone line. The modem connects to the Internet by dialing a telephone number at the Internet Service Provider's site. This is in distinction to other connection methods, such as Digital Subscriber Lines, that do not use analog modems and do not dial telephone numbers.

HARD DRIVE ENCRYPTION

Hard Drive Encryption makes everything on your computer unreadable to unauthorized users, and an encryption username and password are required before your computer fully boots up. This prevents hackers from breaking into your operating system by removing your disk and using bypass tools or alternative boot media. Your full hard disk is encrypted, including deleted and

temporary files, which protects your sensitive data if your disk is stolen or lost.

DLL (DYNAMIC LINK LIBRARY)

A library of functions that can be accessed dynamically (that is, as needed) by a Windows application.

DNS (DOMAIN NAME SERVER)

A data query service generally used on the Internet for translating host names or domain names (like www.yoursite.com) into Internet addresses (like 123.456.789.0).

DRIVER

A program that controls a device. In Windows environments, drivers often have a.DRV extension. A driver acts like a translator between the device and programs that use the device. Each device has its own set of specialized commands that only its driver knows. In contrast, most programs access devices by using generic commands. The driver accepts generic commands from a program and then translates them into specialized commands for the device.

EMBEDDED OBJECT

An object such as a sound file or an image file that is embedded in a Web page.

ENCRYPTION

The process of transmitting scrambled data so that only authorized recipients can unscramble it. For instance, encryption is used to scramble credit card information when purchases are made over the Internet.

FOREIGN LANGUAGE FILTERS

A feature of ZoneAlarm security software's junk e-mail filter. Foreign language filters block e-mail containing non-European languages.

GAME MODE

Game Mode temporarily suppresses most ZoneAlarm security software scans, product updates, and alerts, so that you can play games on your computer with fewer interruptions. Game Mode lets you temporarily allow or deny all program permission requests, so that ZoneAlarm security software can answer such requests automatically without displaying alerts.

GATEWAY

In networking, a combination of hardware and software that links two different types of networks. For example, if you are on a home or business Local Area Network (LAN), a gateway enables the computers on your network to communicate with the Internet.

HASH

A hash is a number generated by a formula from a string of text in such a way that it is unlikely that some other text would produce the same value. Hashes

are used to ensure that transmitted messages have not been tampered with.

HEARTBEAT MESSAGES

Messages sent by an Internet Service Provider (ISP) to make sure that a dial-up connection is still in use. If it appears a customer is not there, the ISP might disconnect her so that her IP address can be given to someone else.

HIGH-RATED ALERTS

An alert that is likely to have been caused by hacker activity. High-rated Firewall alerts display a red band at the top of the alert pop-up. In the Log Viewer, you can see if an alert was high-rated by looking in the Rating column.

HTTP REFERRER HEADER FIELD

An optional field in the message that opens a Web page, containing information about the "referring document." Properly used, this field helps Web masters administer their sites. Improperly used, it can divulge your IP address, your workstation name, login name, or even (in a poorly-implemented e-commerce site) your credit card number. By selecting Remove Private Header information in the Cookies panel, you prevent this header field from transferring any information about you.

ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

An extension of the Internet Protocol that supports error control and informational messages. The "ping" message is a common ICMP message used to test an Internet connection.

ICS (INTERNET CONNECTION SHARING)

ICS is a service provided by the Windows operating system that enables networked computers to share a single connection to the Internet.

INDEX.DAT

Index.dat files keep copies of everything that was in your Temporary Internet, Cookies, and History folders even AFTER these files have been deleted.

INFORMATIONAL ALERTS

The type of alerts that appear when ZoneAlarm security software blocks a communication that did not match your security settings. Informational alerts do not require a response from you.

INTERNET ZONE

The Internet Zone contains all the computers in the world—except those you have added to the Trusted Zone or Blocked Zone.

ZoneAlarm security software applies the strictest security to the Internet Zone, keeping you safe from hackers. Meanwhile, the medium security settings of the Trusted Zone enable you to communicate easily with the computers or networks you know and trust—for example, your home network PCs, or your

business network.

IP ADDRESS

The number that identifies your computer on the Internet, as a telephone number identifies your phone on a telephone network. It is a numeric address, usually displayed as four numbers between 0 and 255, separated by periods. For example, 172.16.100.100 could be an IP address.

Your IP address may always be the same. However, your Internet Service Provider (ISPs) may use Dynamic Host Configuration Protocol (DHCP) to assign your computer a different IP address each time you connect to the Internet.

ISP (INTERNET SERVICE PROVIDER)

A company that provides access to the Internet. ISPs provide many kinds of Internet connections to consumers and business, including dial-up (connection over a regular telephone line with a modem), high-speed Digital Subscriber Lines (DSL), and cable modem.

JAVA APPLET

A small Internet-based program written in Java that is usually embedded in an HTML page on a Web site and can be executed from within a browser.

JAVASCRIPT

A popular scripting language that enables some of the most common interactive content on Web sites. Some of the most frequently used JavaScript functions include Back and History links, changing images on mouse-over, and opening and closing browser windows. ZoneAlarm security software default settings allow JavaScript because it is so common and because most of its uses are harmless.

KEYLOGGER

A form of spyware that records keystrokes on your computer, often sending the data to a remote server. Any text input using the keyboard, including credit card numbers or other sensitive personal information could be gathered by a keylogging program and used to commit identity theft.

MAIL SERVER

The remote computer from which the e-mail program on your computer retrieves e-mail messages sent to you.

MD5 SIGNATURE

A digital "fingerprint" used to verify the integrity of a file. If a file has been changed in any way (for example, if a program has been compromised by a hacker), its MD5 signature will change as well.

MEDIUM-RATED ALERT

An alert that was probably caused by harmless network activity, rather than by

a hacker attack.

MESSAGE FILTERS

A feature of ZoneAlarm security software's junk e-mail filter. Message Filters use heuristic rules to analyze e-mail for characteristics common to various types of junk e-mail.

MIME-TYPE INTEGRATED OBJECT

An object such as an image, sound file, or video file that is integrated into an e-mail message. MIME stands for Multipurpose Internet Mail Extensions.

MOBILE CODE

Executable content that can be embedded in Web pages or HTML e-mail. Mobile code helps make Web sites interactive, but malicious mobile code can be used to modify or steal data, and for other malevolent purposes.

MOBILE CODE CONTROL

A ZoneAlarm security software feature that enables you to block active controls and scripts on the Web sites you visit. While mobile code is common on the Internet and has many benign uses, hackers can sometimes use it for malevolent purposes.

NETBIOS (NETWORK BASIC INPUT/OUTPUT SYSTEM)

A program that allows applications on different computers to communicate within a local network. By default, ZoneAlarm security software allows NetBIOS traffic in the Trusted Zone, but blocks it in the Internet Zone. This enables file sharing on local networks, while protecting you from NetBIOS vulnerabilities on the Internet.

OPENSSL

OpenSSL is an open source security protocol based on the SSL library developed by Eric A. Young and Tim J. Hudson.

PACKET

A single unit of network traffic. On "packet-switched" networks like the Internet, outgoing messages are divided into small units, sent and routed to their destinations, then reassembled on the other end. Each packet includes the IP address of the sender, and the destination IP address and port number.

PASS-LOCK

When the Internet Lock is engaged, programs given pass-lock permission can continue accessing the Internet. Access permission and server permission for all other programs is revoked until the lock is opened.

PERSISTENT COOKIE

A cookie put on your hard drive by a Web site you visit. These cookies can be retrieved by the Web site the next time you visit. While useful, they create a vulnerability by storing information about you, your computer, or your

Internet use in a text file.

PERVASIVENESS
Pervasiveness refers to a virus' potential to spread. A boot sector virus that spreads through the manual sharing of floppy disks is given a low Pervasiveness rating, while a worm that has the ability to send itself out to a large number of victims is given a high pervasiveness rating.

PHISHING
The act of sending a deceptive e-mail that falsely claims to be from a legitimate business or agency. A phishing e-mail attempts to deceive recipients into providing personal information that can then be used for fraudulent purposes.

PHYSICAL MEMORY
The memory hardware (normally RAM) installed in a computer.

PING
A type of ICMP message (formally "ICMP echo") used to determine whether a specific computer is connected to the Internet. A small utility program sends a simple "echo request" message to the destination IP address, and then waits for a response. If a computer at that address receives the message, it sends an "echo" back. Some Internet providers regularly "ping" their customers to see if they are still connected.

POP-UNDER AD
An ad that appears in a new browser window that opens under the window you're looking at, so you don't see the ad until you close the original browser window.

POP-UP AD
An ad that appears in a new browser window that 'pops up' in front of the window you're looking at.

PORT
A channel associated with the use of TCP or UDP. Some ports are associated with standard network protocols; for example, HTTP (Hypertext Transfer Protocol) is traditionally addressed to port 80. Port numbers range from 0 to 65535.

PORT SCAN
A technique hackers use to find unprotected computers on the Internet. Using automated tools, the hacker systematically scans the ports on all the computers in a range of IP addresses, looking for unprotected or "open" ports. Once an open port is located, the hacker can use it as an access point to break in to the unprotected computer.

PRIVATE NETWORK
A home or business Local Area Network (LAN). Private networks are placed

in the *Trusted Zone* by default.

PRODUCT UPDATE SERVICE
ZoneAlarm subscription service that provides free product and virus signature updates to ZoneAlarm security software. When you purchase ZoneAlarm security software, you automatically receive a year's subscription to product update service. This way you always have the latest version of the product and can detect newly created viruses as well.

PROGRAMS LIST
The list of programs to which you can assign Internet access and server permissions. The list is shown in the Programs panel of the Program Control panel. You can add programs to the list, or remove programs from it.

PROTOCOL
A standardized format for sending and receiving data. Different protocols serve different purposes; for example SMTP (Simple Mail Transfer Protocol) is used for sending e-mail messages; while FTP (File Transfer Protocol) is used to send large files of different types. Each protocol is associated with a specific port, for example, FTP messages are addressed to port 21.

PUBLIC NETWORK
A large network, such as that associated with an ISP. Public networks are placed in the *Internet Zone* by default.

QUARANTINE
A method used to render harmless suspicious attachments, viruses, or spyware.

SCRIPT
A series of commands that execute automatically, without the user intervening. These usually take the form of banners, menus that change when you move your mouse over them, and pop-up ads.

SECURITY LEVELS
The High, Med., and Off settings that dictate the type of traffic allowed into or out of your computer.

SELF-SIGNED CERTIFICATE
A public-key certificate for which the public key bound by the certificate and the private key used to sign the certificate are components of the same key pair, which belongs to the signer.

SERVER PERMISSION
Server permission allows a program on your computer to "listen" for connection requests from other computers, in effect giving those computers the power to initiate communications with yours. This is distinct from access permission, which allows a program to initiate a communications session with

another computer.

SESSION COOKIE

A cookie stored in your browser's memory cache that disappears as soon as you close your browser window. These are the safest cookies because of their short life-span.

SHA1

An algorithm used for creating a hash of data.

SKYSCRAPER AD

An ad that appears in a vertical column along the side of a Web page.

SMARTDEFENSE ADVISOR

ZoneAlarm SmartDefense Advisor is an online utility that enables you to instantly analyze the possible causes of an alert, and helps you decide whether to respond Allow or Deny to a Program alert. To use SmartDefense Advisor, click the More Info button in an alert pop-up. ZoneAlarm security software sends information about your alert to SmartDefense Advisor. SmartDefense Advisor returns an article that explains the alert and gives you advice on what, if anything, you need to do to ensure your security.

SPAM

An inappropriate attempt to use a mailing list or USENET or other networked communications facility as if it were are broadcast medium by sending unsolicited messages to a large number of people.

STEALTH MODE

When ZoneAlarm security software puts your computer in stealth mode, any uninvited traffic receives no response--not even an acknowledgement that your computer exists. This renders your computer invisible to other computers on the Internet, until permitted program on your computer initiates contact.

TCP (TRANSMISSION CONTROL PROTOCOL)

One of the main protocols in TCP/IP networks, which guarantees delivery of data, and that packets are delivered in the same order in which they were sent.

THIRD PARTY COOKIE

A persistent cookie that is placed on your computer, not by the Web site you are visiting, but by an advertiser or other "third party." These cookies are commonly used to deliver information about your Internet activity to that third party. Also known as tracking cookies.

TROJAN HORSE

A malicious program that masquerades as something useful or harmless, such as a screen saver. Some Trojan horses operate by setting themselves up as servers on your computer, listening for connections from the outside. If a hacker succeeds in contacting the program, he can effectively take control of your computer. This is why it's important to only give server permission to programs you know and trust. Other Trojan horses attempt to contact a

remote address automatically.

TRUEVECTOR SECURITY ENGINE

The primary component of ZoneAlarm security software security. It is the TrueVector engine that examines Internet traffic and enforces security rules.

TRUSTED ZONE

The Trusted Zone contains computers you trust and want to share resources with.

For example, if you have three home PCs that are linked together in an Ethernet network, you can put each individual computer or the entire network adapter subnet in the ZoneAlarm security software Trusted Zone. The Trusted Zone's default medium security settings enable you to safely share files, printers, and other resources over the home network. Hackers are confined to the Internet Zone, where high security settings keep you safe.

UDP (USER DATAGRAM PROTOCOL)

A connection-less protocol that runs on top of IP networks and is used primarily for broadcasting messages over a network.

WEB BUG

An image file, often 1x1 pixel, designed to monitor visits to the page (or HTML e-mail) containing it. Web bugs are used to find out what advertisements and Web pages you have viewed.

WILD

Refers to a virus that is spreading as a result of normal day-to-day operations on and between the computers of unsuspecting users. The Wild rating refers to the number of customer reports about this virus. A low Wild rating will reflect a low number of customer reports, whereas a Medium or High Wild rating will reflect a more substantial number of customer reports.

Index

A

access permission
  and anti-virus software 206
  browser software and 206
  configuring for programs 12
  e-mail programs and 207
  for Trusted Zone 11
  FTP programs and 208
  games and 208
  granting to programs 31, 92
  setting for ports 44
act as server 11
  defined 222
Action
  in expert rule 48, 55
  in Log Viewer 42, 187
activist sites, blocking 144
adding
  custom ports 44
  expert rules to programs 111
  networks to the Trusted Zone 38
  programs to the programs list 105
  to the Blocked Zone 42
  to the Trusted Zone 40
  wireless networks to the Internet Zone 39
Additional Services 5
Address 53
Address Mask Reply and Request 53
Address Resolution Protocol, enabling 37
adult content, blocking 142
Advanced Program alert 73
Advanced Program Control 95
alerts
  high-rated 61
  ID Lock 82
  Informational 60
  Internet Lock 64
  logging of 182
  medium-rated 61
  New Network 83, 85
  OSFirewall 75
  Program
    Advanced Program alert 73
    Automatic VPN Configuration alert 28, 74
    Blocked Program 63
    Changed Program alert 69
    Manual Action Required alert 74
    New Program 68, 75, 81
    Repeat Program alert 185
    Server Program alert 64, 92, 185, 206
  reference ??–85
  responding to 8, 28
  stopping them while gaming 195
Alt 52
Amazon protection profile, creating 17
answering machine programs 207
antivirus protection
  status, viewing 135
antivirus protection feature 120–??
AOL
  in expert rules 52
  Instant Messager, using 206
Application Interaction 108
Application Interaction Control 95
archive files
  viruses and 132
asterisks, use of 165
Authenticating Header (AH) Protocol 28
Auto control setting 95
Auto-Learn 94
Auto-learn 95
Auto-learn security setting
  program control and 94
automatic lock
  enabling 98
  setting options for 99
Automatic VPN Configuration alert 74

B

backing up and restoring security settings 15
Blocked Program alert 63
Blocked Zone
  about 10
  adding to 42
blocking
  inappropriate Web content 142–145
  packet fragments 37
  ports 43–45
  programs 37
  Web content by category 139–145
Blue Coat 139, 140
Blue Coat, mentioned 139
browser cache, cleaning 145
browser defaults, modifying 77
browser security 117
browser software, using 206

C

categories
  allowing and blocking 140, 141—145
Cerberian, mentioned 139
Challenged Mail 156
Changed Program alert 69
Changes Frequently 106
chat programs
  Server Program alert and 206
  using 206
check for update settings 14
clear text password 83
closing the ZoneAlarm security software application 7
code injection *see suspicious behavior*
  types of 80
collaborative filter 154
color-scheme, changing 16, 17
COM protection 97
component control 95
components
  managing 110
  VPN-related 28
Components List 110
Configuration Wizard 12
contextual scan 129
contributing fraudulent e-mail 153
contributing junk e-mail 152
Control Center,overview 1—??
CreateProcess 108
custom ports, adding 44

D

Date/Time
  in Log Viewer 187
Day/Time
  adding to expert rule 49
  ranges, creating group of 53
decrypting 175
DefenseNet 12
destination
  in expert rules 46, 48, 49
dial-up connection
  configuring 85
disabling
  Windows Firewall 37
disk encryption, stopping 177
disk encryption, uninstalling 177
display preferences, setting 15
Domain Name Server (DNS)
  defined 225
  in expert rules 52
  incoming messages
    determining source of 187
  outgoing messages
    default port permissions for 43
    determining destination of 43, 187
  required VPN resources 30
  troubleshooting Internet connection 202
Driver event 101
drivers, loading 80
Dynamic Host Configuration Protocol (DHCP) messages
  default port permissions for 43
  in Day/Time group 52
  remote control programs and 210
Dynamic Real-time rating (DRTR) 141

E

eBay protection profile, creating 17
EBay, blocking 143
echo request
  in expert rules 52
e-mail
  fraudulent, reporting 153
  junk, reporting 152
E-mail Filter toolbar 150
e-mail protection 147—149
  about 147
  outbound 148
Encapsulating Security Payload (ESP) protocol
  VPN protocols and 28, 37
event logging
  about 182
  customizing 185
  turning on and off 183
excluding a process from scans 128
Execution event 101
expert firewall rules
  about 46
  creating 48—49
  editing 56
  enforcement of 46—47
  for programs 111
  managing 54—56
  ranking 55
  tracking options for 55
expired, license 18

F

false positive detections 203
false positives 203
file and printer sharing
  enabling 26, 84
  network security and 38
  server access and 72
  troubleshooting 207
File event 101
file-specific scan 129
filter options, setting 109
filtering Web content 141

Firewall alert
determining source of 62
logging of 185
responding to 61
Firewall alerts 61
firewall protection 33—56
about 33
advanced security options 35—41
blocking and unblocking ports 43
expert rules and 46—47
setting security level for 34—35
FireWire 37
ForceField 117
ForceField Help 118
foreign language filters 154
formatting log file 184
fragments, blocking 37
fraudulent e-mail, see junk e-mail filter
Fraudulent Mail folder 153
FTP
programs, using 208
protocols, adding to expert rules 52

G

Game Mode 195
games
online, blocking access to 143
stopping alerts while playing 195
using with ZoneAlarm security software 208—209
gaming software
suspicious behavior and 80
gateway
adding to the Trusted Zone 40
as Location type 51
forwarding or suppressing alerts 36
Internet Connection Sharing (ICS) and 27
default port permissions 43
security enforcement of 36
Generic Routing Encapsulation (GRE) protocol
mentioned 37
VPN protocols and 28, 31
glamour and lifestyle sites, blocking 143
government sites, blocking 143
groups
adding to expert rules 50—54

H

Hacker ID
about 191
handle protection 95
hard drive encryption, troubleshooting 205
heartbeat messages
allowing 201
defined 226
dial-up connection, troubleshooting 201
heuristic scanning 125
heuristics 120
hibernation 173
High security setting
about 10
alert events shown in 183
allowing uncommon protocols 31
default port permissions in 43—44
file and printer sharing 26
firewall protection and 35
for ID Lock 163
for Internet Zone 35
for Trusted Zone 35
logging options and 183
program control and 94
high-rated alerts 61
High-rated Suspicious Behavior alert 77
home network
Firewall alerts and 62
host file, locking 37
host name
adding to Trusted Zone 200
in list of traffic sources 39
Hotmail, special folders 150, 158
humor sites, blocking 143
Hypertext Transfer Protocol (HTTP)
in expert firewall rules 52

I

ID Lock 160—168
overview 160
ID Lock alert 82
Identity Protection Center 160, 168
identity theft
protection from 160, 168
IGMP
default port permissions for 43
in expert rules 46, 112
IMAP4
in expert rules 52
infected files
risk assessment of 131
Information reply 53
Information request 53
Informational alerts 60
Internet auction sites, blocking 143
Internet Connection Sharing (ICS)
alert options for 65
enabling 27
setting security options for 35—36
Internet Control Messaging Protocol (ICMP)
default port permissions for 43
in expert firewall rules 46
message types 52
troubleshooting Internet connection 202
Internet Explorer
granting access permission to 206
Internet Key Exchange (IKE) protocol
VPN protocols and 28

Internet Lock 7
  icon 7
Internet Lock alerts 64
Internet Service Provider (ISP)
  heartbeat messages from 8, 201
  in alert details 84
  in list of traffic sources 39
Internet Zone
  adding networks to automatically 38, 39
  networks, adding to automatically 23
  permissions and 11
IP address
  adding to the Trusted Zone 26, 27, 40
  determining network type from 24, 25
  hiding in submissions to Zone Labs 17
  in expert rules 46
  in list of traffic sources 39
IP Security (IPSec) protocol
  VPN protocols and 28

J

junk e-mail filter
  and privacy 156
  automatic reporting option 157
  blocking company names 151
  blocking mailing lists 152
  blocking senders 151
  Challenged Mail folder 156
  collaborative filter 154
  contributing junk e-mail 152
  foreign language filters 154
  Fraudulent Mail folder 153
  Hotmail, and 150, 158
  Junk Mail folder 153
  message filtering options 154
  message filters 154
  protecting privacy 152, 153, 154
  reporting fraudulent e-mail 153, 157
  reporting junk e-mail 152
  reports 158
  special Outlook folders 150—158
  toolbar 150
  wireless device support 157
Junk E-mail Filter, see junk e-mail filter 150
Junk Mail folder 153

K

keyboard and mouse
  monitoring 79
keyboard shortcuts 215—220
killing a program 105
known issues x

L

Layer 2 Tunneling protocol (L2TP)
  VPN protocols and 28
license key
  updating 19
license key, changing 19
license, expiration 18
Lightweight Directory Access protocol (LDAP)
  VPN protocols and 28
local servers, blocking 37
Location 50
locations
  adding to expert firewall rules 49
  creating groups of 50
lock icon
  in System Tray 7
lock mode, specifying 99
log entries
  about 182
  archiving 190
  expert rules and 112
  fields in 189
  for Program alerts 185
  for programs 185
  formatting 184
  options for 185
  viewing 186, 188
Log Viewer
  accessing 186
Lookup button 50
loopback adaptor
  adding to the Trusted Zone 28
Low security setting
  Changes Frequently option 106
  default port permissions for 43—44
  file and printer sharing and 35
  program control and 94
  Zones and 34
lsass.exe 9

M

mail servers, connecting to 27
MailFrontier 152
MailSafe alert 62
manual file scan 129
MD5 Signature 106
  defined 227

Medium security setting
about 10
alert events 183
alerts and 62, 71
customizing 11
default port permissions for 43—44
file and printer sharing and 26
ID Lock and 163
Internet Zone and 34, 202, 207
logging options and 183
networking and 27
port access and 44
program control and 94, 207
resource sharing and 200
Trusted Zone and 34, 40, 199
uncommon protocols and 37
medium-rated alerts 61
Message event 101
message filters 154
Microsoft Catalog Utilization 95
military sites, blocking 143
mime-type integrated objects
defined 228
Min security setting
program control and 94
Module event 101
More Info button 61, 66, 72, 76, 78, 82
keyboard shortcut for 220
MP3 sites, blocking 143
My Computer 48
myVAULT 163—166
adding data to 163
editing and removing data 165

N

NetBIOS
default port permissions for 44
defined 228
firewall alerts and 62
heartbeat messages and 201
High security setting and 35
in expert firewall rules 52
network visibility and 199
Network Configuration Wizard
about 24
disabling 24, 25
Network News Transfer Protocol (NNTP) 52
network resources, sharing 23
network security options, setting 38
network settings
setting 38
New Network alert 83, 85
New Program alert 68, 75, 81
news and media sites, blocking 144

O

on-demand scan 129
OpenGL
and system crash 209
OpenProcess 108
OSFirewall
configuration 96
OSFirewall events
types of 101
Outbound MailSafe protection
customizing 148—149
enabling 148
Outlook, and junk e-mail filter 150

P

packet
defined 228
expert firewall rules 46
in alerts 61
source of
determining 189
types, blocking 36
parameter problem
in expert rules 52
Parental Control ??—145
about 139
allowing and blocking categories 141—145
enabling 139, 140
setting preferences for 141
setting timeout options for 140
Smart Filtering and 140
Parental Controls 139
pass-lock permission
granting to a program 109
passwords
creating 13
VNCviewer and 210
pay-to-surf sites, blocking 144
PC Anywhere
suspicious behavior and 80
PCAnywhere *see* remote control programs, using
permission
pass-lock 7, 98
passwords and 14
server 11
phishing 153
Physical Memory event 101
physical memory, changes to *see suspicious*
types of 80
ping messages
allowing in Internet Zone 201
and alerts 61
default port permissions for 43
Point-to-Point Tunneling Protocol (PPTP)
VPN protocols and 28
policy 98

POP3
in expert firewall rules 52
ports
1394 37
adding 44
blocking and unblocking 43—44
default permissions for 44
firewall protection and 34
High security setting and 35
in expert firewall rules 46
preferences
for firewall protection 36
for Parental Control 141
keyboard shortcut 218
load at startup 201
preferences, setting 15
printers *see* network resources, sharing
private network
defined 229
Network Configuration Wizard and 24
virtual *see* Virtual Private Network (VPN)
Process event 101
product updates 20
product updates and upgrades 5
Program alerts 65—73
responding to 98
Program Component alert 70
program components
managing 110—111
Program Control 89—209
about 89
Internet Lock and 99
setting level for 93
Zones and 11
program permissions 104
programs
adding to the programs List 105
creating expert rules for 111
stopping 105
trust level of 105
programs list
accessing 102
adding and removing programs 105
protection statistics 5
protocols
creating group of 51
default permissions for 43
firewall protection and 36
in expert firewall rules 46
in expert rules 37
mail 27
VPN 28, 31
proxy server
avoidance systems, blocking access to 143
troubleshooting Internet Connection 200
public network
defined 230
Network Configuration Wizard and 24

Q

quarantine, false positive 203
quarantine, troubleshooting 203

R

range of IP addresses
adding to the Trusted Zone 41
in expert firewall rules 48
ranking expert firewall rules 47, 55
Real Networks
in expert firewall rules 52
recovery disk, full disk encryption 175
recovery media, creating 175
redirect 52
Registry event 101
remote control programs, using 209
remote host computers
VPN configuration and 30
remove disk encryption 177
Repeat Program alert 69
logging options and 185
reporting
fraudulent e-mail 153
junk e-mail 152
responding to alerts 8, 28
restoring security settings 15
restricting program access 105
risk assessment of infections 131
riskware 127
router advertisement 52
router solicitation 52
RTSP 52

S

scan mode 124
scan, on-demand 129
scanning for viruses ??—132
scanning for viruses and spyware 129—??
schedule scans 121
Secure Hypertext Transfer Protocol (HTTPS) 52
secured wireless network
Wireless Network Configuration Wizard and 25
security settings
backing up and restoring 15
sharing with Zone Labs *see* DefenseNet
send mail permission 107
Outbound MailSafe protection and 148

server permission
alerts and 71
chat programs and 206
column in programs list 105
default for traffic types 43
e-mail programs and 207
expert rules and 111
file sharing programs and 207
games and 208
granting to programs 106
streaming media programs and 210
Voice Over Internet programs and 211
Zones and 11
Server Program alert 64, 92, 206
logging options and 185
server, program acting as 90
service control 96
services control 96
services.exe 9
shortcut menu 7
SKIP 28
Smart Filtering
about 139
enabling 139
SmartDefense 104
SmartDefense Advisor 62
about 191
browser permission and 72
defined 231
setting level for 98
submitting alerts to 66, 82
SMTP
in expert firewall rules 52
software rendering mode 208
source
in expert firewall rules 46
of traffic, determining 39, 182
spoolsv.exe 9
spyware
preventing 102
Status tab 4
stealth mode
defined 231
High security setting and 35
Stop button 7
system tray icon 7
subnet
adding to the Trusted Zone 40
entry type 40
VPN configuration and 30
subscription 5
Super access 105
supported hardware and software x
Suspicious Behavior alert 75
svchost.exe 9
system requirements x

T

Telnet 52, 210
TFTP 52
Timbuktu *see* remote control programs, using
time exceeded 52
Timestamp, Timestamp reply 53
timing attack prevention 95
toolbar, E-mail Filter 150
traceroute 53
tracking options
for expert firewall rules 48, 55
traffic sources
default port permissions for 43
list of 39
managing 39
Transmission Control Protocol (TCP)
default port permission for 44
in expert firewall rules 46
treating viruses 126
Trojan 92
Trojan horse 92
e-mail protection and 147
Program Control and 106
Troubleshooting 197—202
TrueVector security engine 201
Trust Levels 104, 105
Trusted access 105
Trusted Sites list 166—168
Trusted Zone
adding networks to automatically 38
adding to 40
Internet Connection Sharing (ICS) and 27
networks, adding to automatically 23
permissions and 11
VPN resources, adding to 28

U

UDP
default port permissions for 44
in expert firewall rules 46
Uninstalling ZoneAlarm 21
unsecured wireless network
Wireless Network Configuration Wizard and 25
updates, automatic antivirus 121
updating software 14
updating ZoneAlarm 20
User Forum x

V

video software
suspicious behavior and 80
violent content, blocking 145

Virtual Private Network (VPN)
alerts 28, 74
Automatic Configuration alert 74
configuring connection 27—31, 198
Manual Action Required alert 74
troubleshooting connection 197
virtualization 118
viruses
and archive files 132
scanning for 129—132
treating 126, 131
updating signature files 121
VNC
suspicious behavior and 80
VNC programs, using 210
VoIP programs, using 211

W

Web conferencing programs, using 211
web content, filtering 109
Who Is tab *see* Hacker ID
Windows Firewall, disabling 37
Windows Media
in expert rules 52
winlogon.exe 9
wireless network security options, setting 39
wireless network settings
setting 39

Z

Zone Alarm Fraudulent Mail, see junk e-mail filter
Zone Alarm Junk Mail, see junk e-mail filter, special Outlook folders
Zone Labs security software
file sharing programs and 207
FTP programs and 208
loading at startup 16
updating 14
ZoneAlarm Challenged Mail, see junk e-mail filter
ZoneAlarm security software
about 7
closing the application 7
Zones
about 10
adding to 40—41
firewall protection and 39